goEntry™

Manual del Usuario del Software

INNOVACIÓN PERPÉTUA



Lenel® Manual del Usuario del Software goEntry™, versión del producto 3.00. Este manual es el artículo número 460815001, revisión A de Junio de 2012

Fabricante

Lenel Systems International, Inc., 1212 Pittsford-Victor Road, Pittsford, NY 14534-3820, EE. UU.

Representante autorizado de fabricación en la UE:
UTC Fire & Security B.V.
Kelvinstraat 7, 6003 DH Weert, Países Bajos

Versión

Este documento se aplica a la versión 3.0 de goEntry

Certificación

CE N4131

Conformidad FCC

Este dispositivo cumple con la parte 15 de las Normas de la FCC. La operación está sujeta a las siguientes condiciones: (1) Este dispositivo no puede causar interferencias perjudiciales y (2) este dispositivo debe aceptar cualquier interferencia que reciba, incluidas interferencias que pueda causar un funcionamiento no deseado.

Conformidad FCC Clase A

Se ha comprobado que este equipo cumple los límites para dispositivos digitales de clase A, de acuerdo con la parte 15 de las Normas de la FCC. Estos límites han sido establecidos para proporcionar una protección razonable contra interferencias perjudiciales cuando el equipo funciona en un entorno comercial. Este equipo genera, usa y puede irradiar energía de radiofrecuencia y, si no se instala y usa de acuerdo con el manual de instrucciones, puede causar interferencias perjudiciales en las comunicaciones de radio. El funcionamiento de este equipo en un área residencial puede causar interferencias perjudiciales, en cuyo caso el usuario deberá corregir la interferencia por sus propios medios.

Conformidad FCC Clase B

Se ha comprobado que este equipo cumple los límites para dispositivos digitales de clase B, de acuerdo con la parte 15 de las Normas de la FCC. Estos límites han sido

establecidos para proporcionar una protección razonable contra interferencias perjudiciales en una instalación residencial. Este equipo genera, usa y puede irradiar energía de radiofrecuencia y, si no se instala y usa de acuerdo con las instrucciones, puede causar interferencias perjudiciales en las comunicaciones de radio.

No hay garantía de que no se produzcan interferencias en una instalación particular. Si este equipo causa interferencias perjudiciales en la recepción de radio o televisión, lo cual puede determinarse apagando y prendiendo el equipo, se recomienda al usuario que intente corregir la interferencia tomando las siguientes medidas:

- Reorientar o reubicar antena de recepción.
- Aumentar la distancia entre el equipo y el receptor.
- Conectar el equipo a un tomacorriente de un circuito diferente al que está conectado el receptor.
- Consultar al distribuidor o técnico de radio/TV para obtener ayuda.

Conformidad con ACMA

¡Aviso! Es un producto Clase A. En un entorno doméstico este producto puede causar interferencias de radio, en cuyo caso el usuario deberá tomar las medidas adecuadas.

Canadá

Este aparato digital Clase A cumple con la norma canadiense ICES-003. Cet appareil numérique de la classe A est conforme à la norme NMB-0330 du Canada.

Directivas Unión Europea

2004/108/CE (Directiva CEM): Por la presente, Lenel declara que este dispositivo cumple con los requisitos esenciales y otras disposiciones pertinentes de la Directiva 2004/108/CE.



2002/96/CE (Directiva RAEE): En la Unión Europea, los productos marcados con este símbolo no se pueden descartar entre los residuos municipales sin clasificar. Para su correcto reciclaje, devolver este producto a su proveedor local al comprar un nuevo equipo equivalente, o entregarlo en puntos especiales de recolección. Para obtener más información entrar en: www.recyclethis.info.



2006/66/CE (directiva relativa a las pilas): Este producto contiene una pila que, en la Unión Europea, no se puede desechar entre los residuos municipales sin clasificar. Consultar la documentación del producto para obtener información específica sobre la pila. La pila está marcada con este símbolo, que puede incluir letras para indicar que contiene cadmio (Cd), plomo (Pb) o mercurio (Hg). Para su correcto reciclaje, devolver la batería a su proveedor o entregarla en un punto de recolección. Para obtener más información entrar en: www.recyclethis.info.

Información de contacto	www.lenel.com
Atención al cliente	www.lenel.com/support

Licencias públicas GNU

Linux Kernel 2.6.30, Pthreads, Larry DooLittle, Flex Builder y Buildroot bajo licencia pública general GNU, versión 2. Una copia de la licencia se puede bajar de http://www.gnu.org/licenses/gpl-2.0.html.

YAFFS2 y la tar de GNU bajo licencia pública general GNU, versión 3. Una copia de la licencia se puede bajar de http://www.gnu.org/licenses/gpl-3,0.html.

uClibc, iClibc locale, GPG Gnu Privacy Guard, gpgme GnuPG Made Easy bajo licencia pública general GNU, versión 3. Una copia de la licencia se puede bajar de http://www.gnu.org/licenses/gpl-3,0.html.

OpenSSL, AstraFlex Components and LIGHTTPD están bajo una licencia BSD modificada

LOS TITULARES DE LOS DERECHOS DE AUTOR Y COLABORADORES OFRECEN ESTE PROGRAMA "TAL CUAL", SIN GARANTÍAS DE NINGÚN TIPO, YA SEAN EXPRESAS O TÁCITAS, INCLUIDAS, A TÍTULO ENUNCIATIVO AUNQUE NO LIMITATIVO, LAS GARANTÍAS IMPLÍCITAS DE COMERCIABILIDAD E IDONEIDAD PARA UN FIN ESPECÍFICO. EN NINGÚN CASO LOS AUTORES O COLABORADORES SERÁN RESPONSABLES POR NINGÚN DAÑO DIRECTO, INDIRECTO, INCIDENTAL, ESPECIAL, EJEMPLAR NI CONSECUENTE (INCLUIDA, A TÍTULO ENUNCIATIVO AUNQUE NO LIMITATIVO, LA ADQUISICIÓN DE BIENES Y SERVICIOS SUSTITUTOS, LA PÉRDIDA DE USO, DATOS O GANANCIAS, O LA INTERRUPCIÓN DE LAS OPERACIONES COMERCIALES), SIN IMPORTAR LA CAUSA Y EN CUALQUIER BASE DE RESPONSABILIDAD, YA SEA CONTRACTUAL, RESPONSABILIDAD NO CULPOSA O DAÑO EXTRACONTRACTUAL (POR NEGLIGENCIA O NO) QUE SURJA DE CUALQUIER MODO A PARTIR DEL USO DE ESTE SOFTWARE, INCLUSO SI SE NOTIFICÓ DE LA POSIBILIDAD DE DICHO DAÑO.

CMockery and Google Protocol Buffers (C) están bajo la licencia Apache, Versión 2.0 (en lo sucesivo, la "Licencia")

No se puede usar este archivo excepto de conformidad con la licencia. Se puede obtener una copia de la Licencia en http://www.apache.org/licenses/LICENSE-2.0

A menos que así lo exija la ley aplicable o se acuerde lo contrario por escrito, el software distribuido bajo la Licencia se distribuye "TAL CUAL", SIN GARANTÍAS NI CONDICIONES DE NINGÚN TIPO, ya sean expresas o implícitas. Consultar la Licencia para obtener información sobre las condiciones que rigen los permisos y las limitaciones vigentes en virtud de la Licencia.

Flex-IFrame

Se concede permiso, de forma gratuita, a cualquier persona que obtenga una copia de este software Flex-IFrame y los archivos de documentación asociados (en lo sucesivo el "Software"), para trabajar con el Software sin restricciones, incluidos, sin limitación, los derechos para usar, copiar, modificar, fusionar, publicar, distribuir, sublicenciar y vender copias del Software, y permitir que las personas a quienes se proporcione el Software también lo hagan.

Google Protocol Buffers (C++) está bajo la nueva licencia BSD.

LOS TITULARES DE LOS DERECHOS DE AUTOR Y COLABORADORES OFRECEN ESTE PROGRAMA "TAL CUAL", SIN GARANTÍAS DE NINGÚN TIPO, YA SEAN EXPRESAS O TÁCITAS, INCLUIDAS, A TÍTULO ENUNCIATIVO AUNQUE NO LIMITATIVO, LAS GARANTÍAS IMPLÍCITAS DE COMERCIABILIDAD E IDONEIDAD PARA UN FIN ESPECÍFICO. EN NINGÚN CASO LOS TITULARES DE LOS DERECHOS DE AUTOR O COLABORADORES SERÁN RESPONSABLES POR NINGÚN DAÑO DIRECTO, INDIRECTO, INCIDENTAL, ESPECIAL, EJEMPLAR NI CONSECUENTE (INCLUIDA, A TÍTULO ENUNCIATIVO AUNQUE NO LIMITATIVO, LA ADQUISICIÓN DE BIENES Y SERVICIOS SUSTITUTOS, LA PÉRDIDA DE USO, DATOS O GANANCIAS, O LA INTERRUPCIÓN DE LAS OPERACIONES COMERCIALES), SIN IMPORTAR LA CAUSA Y EN CUALQUIER BASE DE RESPONSABILIDAD, YA SEA CONTRACTUAL, RESPONSABILIDAD NO CULPOSA O DAÑO EXTRACONTRACTUAL (POR NEGLIGENCIA O NO) QUE SURJA DE CUALQUIER MODO A PARTIR DEL USO DE ESTE SOFTWARE, INCLUSO SI SE NOTIFICÓ DE LA POSIBILIDAD DE DICHO DAÑO.

gSOAP está bajo la licencia pública gSOAP (Licencia MPL modificada)

Copyright © 2001-2009 Robert A. van Engelen, Genivia Inc. Todos los derechos reservados.

EL PROGRAMA DE ESTE PRODUCTO FUE PROVISTO, EN PARTE, POR GENIVIA INC, SIN GARANTÍAS DE NINGÚN TIPO, YA SEAN EXPRESAS O TÁCITAS, INCLUIDAS, A TÍTULO ENUNCIATIVO AUNQUE NO LIMITATIVO, LAS GARANTÍAS IMPLÍCITAS DE COMERCIABILIDAD E IDONEIDAD PARA UN FIN ESPECÍFICO. EN NINGÚN CASO EL AUTOR SERÁ RESPONSABLE POR NINGÚN DAÑO DIRECTO, INDIRECTO, INCIDENTAL, ESPECIAL, EJEMPLAR NI CONSECUENTE (INCLUIDA, A TÍTULO ENUNCIATIVO AUNQUE NO LIMITATIVO, LA ADQUISICIÓN DE BIENES Y SERVICIOS SUSTITUTOS, LA PÉRDIDA DE USO, DATOS O GANANCIAS, O LA INTERRUPCIÓN DE LAS OPERACIONES COMERCIALES), SIN IMPORTAR LA CAUSA Y EN CUALQUIER BASE DE RESPONSABILIDAD, YA SEA CONTRACTUAL, RESPONSABILIDAD NO CULPOSA O DAÑO EXTRACONTRACTUAL (POR NEGLIGENCIA O NO)

QUE SURJA DE CUALQUIER MODO A PARTIR DEL USO DE ESTE SOFTWARE, INCLUSO SI SE NOTIFICÓ DE LA POSIBILIDAD DE DICHO DAÑO.

mini_httpd está licenciado bajo la licencia freeware de Acme Labs.

La redistribución y en uso en formato fuente y binario de mini_httpd, con o sin modificaciones, están permitidos siempre que se cumplan las siguientes condiciones:

1. La redistribución del código fuente debe conservar el aviso de copyright anterior, esta lista de condiciones y la siguiente renuncia.
2. Las redistribuciones en formato binario deben reproducir el aviso de copyright anterior, esta lista de condiciones y la siguiente renuncia en la documentación u otros materiales suministrados con la distribución.

EL AUTOR OFRECE ESTE PROGRAMA "TAL CUAL", SIN GARANTÍAS DE NINGÚN TIPO, YA SEAN EXPRESAS O TÁCITAS, INCLUIDAS, A TÍTULO ENUNCIATIVO AUNQUE NO LIMITATIVO, LAS GARANTÍAS IMPLÍCITAS DE COMERCIABILIDAD E IDONEIDAD PARA UN FIN ESPECÍFICO. EN NINGÚN CASO EL AUTOR O LOS CONTRIBUIDORES SERÁN RESPONSABLES POR NINGÚN DAÑO DIRECTO, INDIRECTO, INCIDENTAL, ESPECIAL, EJEMPLAR NI CONSECUENTE (INCLUIDA, A TÍTULO ENUNCIATIVO AUNQUE NO LIMITATIVO, LA ADQUISICIÓN DE BIENES Y SERVICIOS SUSTITUTOS, LA PÉRDIDA DE USO, DATOS O GANANCIAS, O LA INTERRUPCIÓN DE LAS OPERACIONES COMERCIALES), SIN IMPORTAR LA CAUSA Y EN CUALQUIER BASE DE RESPONSABILIDAD, YA SEA CONTRACTUAL, RESPONSABILIDAD NO CULPOSA O DAÑO EXTRACONTRACTUAL (POR NEGLIGENCIA O NO) QUE SURJA DE CUALQUIER MODO A PARTIR DEL USO DE ESTE SOFTWARE, INCLUSO SI SE NOTIFICÓ DE LA POSIBILIDAD DE DICHO DAÑO.

Apache log4Net está bajo la licencia Apache versión 2.0.

Una copia de la licencia se encuentra en http://logging.apache.org/log4net/license.html

Non-English versions of Lenel documents are offered as a service to our global audiences. We have attempted to provide an accurate translation of the text, but the official text is the English text, and any differences in the translation are not binding and have no legal effect.

El software descrito en este documento se suministra bajo un acuerdo de licencia y solo puede usarse de acuerdo con los términos de ese acuerdo.

Microsoft, Windows, Windows XP y Windows 7 son marcas registradas o marcas comerciales de Microsoft Corporation en los Estados Unidos o en otros países. Los otros nombres de productos mencionados en este manual del usuario pueden ser marcas comerciales o marcas registradas de sus respectivas empresas y se reconocen como tales.

El programa de este producto contiene software con derechos de autor que está licenciado bajo la GPL. Se puede obtener todo el código fuente correspondiente durante un período de tres años después de nuestro

último envío de este producto, que será no antes de 2013-08-30, mediante el envío de un giro postal o cheque de $5 dólares a la siguiente dirección:

Lenel
1212 Pittsford-Victor Road
Pittsford, NY 14534-3820

Escribir "source for goEntry" en la línea de memo de su pago. Se puede encontrar una copia de la fuente en http://www.lenel.com. Esta oferta es válida para todos los que reciban esta información.

CAPÍTULO 1 *Introducción* 1

Convenciones usadas en esta documentación 1

CAPÍTULO 2 *Configuración del Hardware goEntry* 3

Arquitectura del Sistema goEntry.. 4

Documentar la ubicación física de cada dispositivo a través del número de serie 5

Conectar el controlador del sistema goEntry a una LAN o estación de trabajo local 6

Configuración de la estación de trabajo cliente local para operar goEntry 7

Instalar Microsoft .NET Framework 4.0. 7

Instalar Servicios de Impresión Bonjour 7

Detección, configuración y puesta a prueba del hardware goEntry 7

Detectar y configurar el hardwaregoEntry 7

CAPÍTULO 3 *Configuración del Software goEntry* 11

Actualizar Firmware Controlador del Sistema goEntry 12

Configurar la fecha y hora 12

Configuración de seguridad de la red... 13

Crear un certificado de seguridad 13

Cargar un certificado de seguridad 14

Habilitar SSL/HTTPS 14

Configuración de seguridad... 14

Configurar la seguridad de las instalaciones 15

Configuración de los formatos de tarjeta.................................... 16

Agregar un formato de tarjeta 16

Eliminar un Formato de tarjeta 16

Formatos de tarjeta por default 16

Configuración de dispositivos 16

Asignar nombres significativos al hardware detectado 17

Configurar goEntry 17

goEntry Entradas y Salidas... 18

Configurar los controladores de puertas 18

Configuración de las puertas 18

Configurar las lectoras 24

Opciones de lectoras 24

Configurar los módulos de expansión de E/S 25

Configuración de dispositivos de video.. 25

Agregar una DVR 26

Añadir una cámara de video 26

Agregar plantillas de video 27

Enlazar las cámaras a los dispositivos de rastreo de videos de eventos 27

Configuración de Áreas... 27

Agregar una área 28

Asignar lectoras a las áreas 28

Eliminar una Área 28

Configurar Anti-passback **29**
Configurar el Anti-passback 29

Creación de grupos de feriados **29**
Agregar un grupo de feriados 30
Agregar un feriado a un grupo de feriados 30
grupo de feriados 30
Eliminar un grupo de feriados 31

Creación de horarios **31**
Agregar un horario 32
Agregar un intervalo a un horario 32
Eliminar un intervalo de un horario 32
Copiar un horario 32
Eliminar un horario 33

Creación de grupos de lectoras **33**
Agregar un grupo de lectoras 33
Copiar un grupo de lectoras 33
Eliminar un grupo de lectoras 33

Configuración de los niveles de acceso **34**
Agregar un nivel de acceso 34
Copiar un nivel de acceso 34
Remover un nivel de acceso 34

Configuración de roles de operador **35**
Agregar un rol de operador 35
Modificar un rol de operador 35
Copiar un rol de operador 35
Eliminar un rol de operador 36

Configuración de Campos definidos por usuario **36**
Añadir campos definidos por usuario 37
Reorganizar campos definidos por usuario 37
Eliminar un campo definido por el usuario 37

Comportamiento programación de puertas y lectoras **37**

Importar personas y credenciales de un archivo CSV **38**

Crear un respaldo y un punto de restauración **38**

CAPÍTULO 4 *Administración de Acceso 39*

Administración de Personas **39**
Agregar una persona 40
Remover una persona 40
Cargar fotos de identificación de la persona 40

Administración de credenciales **41**
Añadir una credencial 41
Lectoras de credenciales USB 41
Remover una credencial 42

Administración de credenciales perdidas o robadas **42**
Evitar el uso de una credencial perdida o robada 42
Restaurar una credencial encontrada 43

Administración de cuentas de usuario **43**
Añadir una cuenta de usuario 43
Cambiar un nombre de usuario y contraseña 44
Desactivar una cuenta de usuario 44

Reportes **44**

Búsqueda de personas 45
Buscar personas *45*
Cancelar la búsqueda *45*

CAPÍTULO 5 *Monitoreo del Acceso* *47*

Eventos y alarmas 47
Ver últimos eventos *48*
Cargar más eventos *48*
Cargar todos los eventos *48*
Búsqueda de Eventos *48*
Exportar eventos *48*
Video de eventos 49
Reproducir video de eventos *49*
Monitorear video *49*
Referencia controles de video *50*
Control de puertas 51
Abrir una puerta *51*
Restablecer una puerta *51*
Bloquear una puerta *51*
Desbloquear una puerta *52*
Restablecer todas las puertas *52*
Bloquear todas las puertas *52*
Desbloquear todas las puertas *52*
Menú Comandos de puertas *52*
Etiqueta Ver eventos *53*
Etiqueta Ver horarios *53*
Modo Puerta degradada *54*
Monitoreo de entradas y salidas 55
Activar o desactivar una salida *55*
Restablecer Anti-passback 55

CAPÍTULO 6 *Mantenimiento* *57*

Iniciar sesión en goEntry 57
Prevención de pérdida de datos 57
Crear una copia de respaldo *58*
Restaurar a partir de un respaldo *58*
Salvar y restablecer la configuración personalizada 58
Salvar los ajustes personalizados *58*
Restablecer ajustes personalizados *58*
Restablecer ajustes de fábrica *59*
Actualización de firmware 60
Reiniciar el controlador del sistema goEntry 60
Página Ajustes del sistema 60
Etiqueta Información del sistema *60*
Etiqueta Fecha y hora *60*
Etiqueta Configuración de red *61*
Etiqueta Seguridad *61*
Etiqueta Campos definidos por el usuario *61*
Descripción de formatos de tarjeta 61

Formatos sin procesar (raw) ... *61*

CAPÍTULO 7 *Solución de problemas* ... *63*

Borrar caché del navegador de Internet ... **63**
Requisitos de visualización ... **63**
Capacidades y limitaciones del sistema ... **64**
Resumen de roles de operador predefinidos ... *65*
Diagnóstico ... **67**
Fusibles ... *69*
Estados problemas de hardware ... *70*
Mensajes error, advertencia y eventos ... **70**
Estados de sabotaje ... *70*
Eventos de alimentación y baterías ... *71*
Eventos batería de respaldo ... *71*
Eventos dispositivos ... *72*
Eventos sabotaje de puerta ... *73*
Eventos de entrada auxiliar ... *73*
Eventos de salida auxiliar ... *73*
Advertencia "Objetos han cambiado" ... *73*
Evento "Error de sinc. NTP" ... *74*
Errores de Active X reproductor de video ... **74**
Ninguna conexión de video activa ... *74*
El navegador de internet no consigue cargar la página Inicio de sesión ... **75**

CAPÍTULO 1 *Introducción*

El software de interfaz de usuario de goEntry™ está incorporado en el controlador del sistema goEntry. goEntry permite:

- Controlar el acceso de hasta 64 puertas, en función de horarios de acceso definidos por el usuario
- Configurar los horarios para incluir feriados recurrentes
- Agregar al sistema hasta 10,000 usuarios y tarjetas ID
- Monitorear los eventos a distancia y automatizar la enlace de los eventos al video correspondiente en las DVRs TruVision
- Abrir, bloquear y restablecer las puertas, a distancia,
- Agregar horarios a las lectoras para ayudar a automatizar el sistema
- Hacer cumplir las reglas Anti-passback
- Crear grupos de lectoras

Convenciones usadas en esta documentación

El texto de este manual está formateado de forma que resulte fácil identificar lo que se describe.

- Cuando un término se define, la palabra está en *cursiva*.
- Los nombres de los campos se muestran en **negrita**.
- Los menús y opciones de menú aparecen en ***negrita y cursiva***. Todas las opciones del menú tienen teclas de aceleración que permiten seleccionar las opciones del menú a través del teclado. La letra subrayada indica la tecla de aceleración correspondiente a la opción de menú. Las teclas de aceleración se escriben, por ejemplo, <Alt>, <C>.
- Las teclas del teclado se presentan entre paréntesis angulares. Por ejemplo: <Tab>, <Ctrl>.
- Las combinaciones de teclas se escriben de dos maneras:

  <Ctrl> + <Z> significa mantener presionada la primera tecla y presionar la segunda

  <Ctrl>, <C> significa presionar la primera tecla y, luego, presionar la segunda
- Los botones de la pantalla se muestran entre corchetes, por ejemplo: [Modificar], [Cancelar].

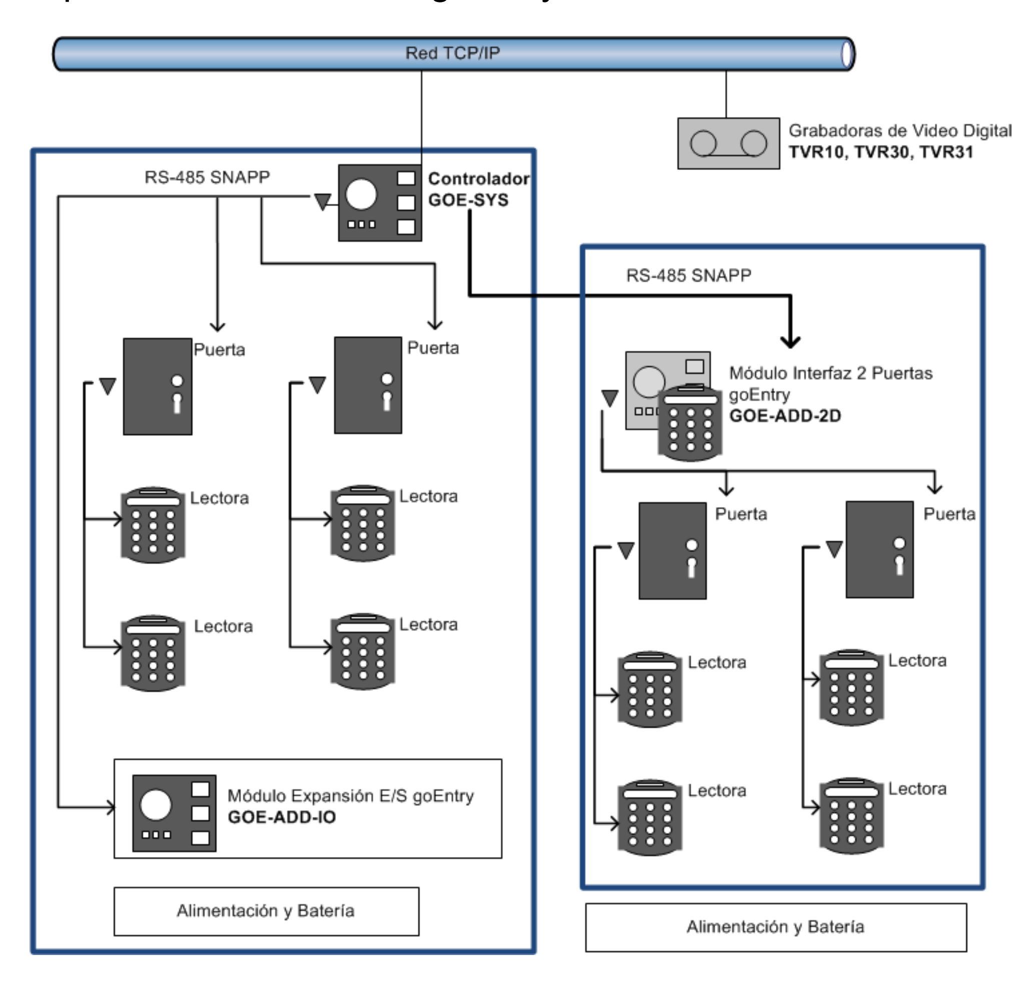
CAPÍTULO 2

Configuración del Hardware goEntry

Una vez instalados los dispositivos de hardware de goEntry, es necesario configurar el controlador del sistema goEntry.

La configuración detallada de las funciones opcionales se realiza en la interfaz de usuario de goEntry. Antes de poder ejecutar esta aplicación, el controlador del sistema goEntry debe conectarse a la red y detectar y probar las entradas, salidas, puertas y lectoras conectadas a él, para comprobar que el cableado y la instalación están correctos.

Arquitectura del Sistema goEntry



Documentar la ubicación física de cada dispositivo a través del número de serie

A medida que se instala la configuración de cada puerta (cerraduras, sensores, lectoras), describir los dispositivos y listar los números de serie correspondientes. Esto será útil más adelante al nombrar los dispositivos, los grupos de lectoras y las zonas, durante la configuración de los dispositivos en la interfaz de usuario de goEntry.

Descripción de la puerta	Número de serie de las lectoras	Controlador de puertas Número de serie	Expansor E/S Número de serie	Cámara enlazada
	Dentro:			
	Fuera:			
	Dentro:			
	Fuera:			
	Dentro:			
	Fuera:			
	Dentro:			
	Fuera:			
	Dentro:			
	Fuera:			
	Dentro:			
	Fuera:			
	Dentro:			
	Fuera:			
	Dentro:			
	Fuera:			
	Dentro:			
	Fuera:			
	Dentro:			
	Fuera:			
	Dentro:			
	Fuera:			
	Dentro:			
	Fuera:			

Descripción de la puerta	Número de serie de las lectoras	Controlador de puertas Número de serie	Expansor E/S Número de serie	Cámara enlazada
	Dentro:			
	Fuera:			
	Dentro:			
	Fuera:			
	Dentro:			
	Fuera:			
	Dentro:			
	Fuera:			
	Dentro:			
	Fuera:			
	Dentro:			
	Fuera:			

Ver **Configuración del Software goEntry en pág. 11.**

Conectar el controlador del sistema goEntry a una LAN o estación de trabajo local

Hay dos tomas ethernet RJ-45 100BaseT en el Controlador de Sistema goEntry. Una de ellas es configurable y la otra tiene una dirección IP (protocolo de internet) fija. Para identificar las tomas, consultar la *Guía de consulta rápida del controlador del sistema goEntry*.

Si se conecta directamente una estación de trabajo cliente local al controlador, usar la toma Ethernet estática y un cable ethernet CAT-6 para hacer la conexión.

Si se conecta el controlador a una red de área local (LAN), usar la toma Ethernet configurable. Consultar con el administrador de la red de las instalaciones sobre la conexión del controlador a la LAN.

Nota: Si se cuenta con varios dispositivos de red con una conexión única a la red a través de un conmutador o un enrutador pequeño, verificar que no haya más que un conmutador o enrutador entre el controlador y la conexión a la red.

Configuración de la estación de trabajo cliente local para operar goEntry

La interfaz de usuario de goEntry se encuentra en el controlador del sistema goEntry, así que todo lo que se necesita para ejecutar la aplicación es un navegador de internet instalado en la estación de trabajo cliente local.

Sin embargo, el Asistente de detección e instalación y el Asistente de importación/exportación se instalan desde un disco en una estación de trabajo local a los efectos de configurar y probar el hardware recién instalado, y cargar en el controlador la base de datos del personal (si procede).

Instalar Microsoft .NET Framework 4.0.

El programa de utilidades de goEntry detecta automáticamente si el programa .NET está instalado y, si lo encuentra, muestra la palabra "instalado" al lado del enlace.

1. Insertar el disco de goEntry en el drive CD/DVD de la computadora.

   Como alternativa, si se descargó la imagen del disco y se la extrajo al disco duro de la computadora, hacer doble clic sobre la aplicación **start.hta** para iniciar el instalador.
2. Hacer clic en **.NET Framework 4.0**.
3. Seguir las instrucciones del instalador de Microsoft .NET para completar la instalación.

Instalar Servicios de Impresión Bonjour

El programa de utilidades de goEntry detecta automáticamente si el programa Bonjour está instalado y, si lo encuentra, muestra la palabra "instalado" al lado del enlace.

1. Insertar el disco de goEntry en el drive CD/DVD de la computadora.

   Como alternativa, si se descargó la imagen del disco y se la extrajo al disco duro de la computadora, hacer doble clic sobre la aplicación **start.hta** para iniciar el instalador.
2. Hacer clic en **Bonjour**.

   La instalación de Servicios Bonjour comienza y termina de forma automática.

Detección, configuración y puesta a prueba del hardware goEntry

Nota: Antes de que el controlador del sistema goEntry pueda ser descubierto por el Asistente de detección e instalación, necesita conectarse a la red de área local.

Detectar y configurar el hardwaregoEntry

1. Insertar el disco de goEntry en el drive CD/DVD de la computadora.

   Como alternativa, si se descargó la imagen del disco y se la extrajo al disco duro de la computadora, hacer doble clic sobre la aplicación **start.hta** para iniciar el instalador.
2. Hacer clic en **Asistente de detección e instalación**.
3. Seleccionar un **Idioma** y hacer clic en [Siguiente].

   El asistente busca en la red todos los controladores del sistema goEntry.

4. Seleccionar el controlador a configurar en la lista y hacer clic en [Siguiente].
5. Escribir la **contraseña** vigente del administrador.

   El **nombre de usuario** predeterminado del administrador es “admin”

   La **contraseña** predeterminada del administrador es "demo"
6. Elegir una nueva contraseña para el administrador.

   IMPORTANTE: La cuenta del administrador tiene acceso a todos los parámetros de configuración de goEntry. Es peligroso mantener el nombres de usuario y la contraseña por defaults. Todos los que están familiarizados con el producto conocen los valores defaults..
7. Escribir la contraseña en los campos **Nueva contraseña** y **Confirmar contraseña**, y hacer clic en [Siguiente].
8. Cambiar la configuración en la etiqueta **Configuración de red**, de acuerdo con las indicaciones del administrador de la red de las instalaciones.

   IMPORTANTE: Los operadores accederán a la interfaz de usuario de goEntry, escribiendo la dirección IP del controlador del sistema goEntry en el campo de dirección del navegador. Si la dirección IP del controlador es dinámica, los operadores de goEntry deben usar una URL virtual u otro alias para acceder al controlador, ya que si la asignación de dirección IP real es cambiada por la red, los operadores no podrán encontrarla.

   IMPORTANTE: HTTPS es muy recomendable. Este protocolo de hipertexto seguro encripta los paquetes entre los navegadores de los usuarios y el controlador e impide que alguien recopile información del usuario espiando el tráfico de la red. Puede haber casos en los que es necesario usar el protocolo de hipertexto no seguro (HTTP). Por ejemplo, si se accede al controlador del sistema goEntry a través de un servidor de red proxy no compatible con HTTPS (SSL), la única opción es deshabilitar HTTPS/SSL.
9. Hacer clic en [Siguiente].

   El asistente detecta los controladores de puertas y los módulos de expansión de E/S conectados al controlador del sistema goEntry.
10. Hacer clic en [Sincronizar con PC] para ajustar la hora correcta en el controlador.
11. Seleccionar las **Terminaciones EOL de entrada global** correctas para indicar cómo están cableados los circuitos antisabotaje y los sensores de las puertas y las lectoras.
12. Para cada entrada auxiliar de uso general que se conecta:
    a. Seleccionar un **Modo**.
    b. Observar las entradas para determinar si están funcionando y comunicándose con el controlador.
13. Para cada salida auxiliar de uso general que se conecta:
    a. Para cambiar el estado, hacer clic en el ícono que se encuentra junto a **Estado**.
    b. Observar las salidas para determinar si están funcionando y comunicándose con el controlador.
14. Para cada controlador de puerta, seleccionar la **Cantidad de puertas** controladas.
15. Para cada puerta:
    a. Seleccionar el **Modo** adecuado de los circuitos de contacto, solicitud de salida y antisabotaje.
    b. Seleccionar los comandos de la lista **Control de puerta** para poner a prueba la instalación y el cableado eléctrico de todas las puertas.

16. Una vez puestos a prueba todos los dispositivos, hacer clic en [Finalizar].

CAPÍTULO 3

Configuración del Software goEntry

goEntry está diseñado para que, una vez configurado, se puedan agregar y eliminar rápidamente personas y credenciales, y administrar el acceso a las instalaciones. Durante la configuración, se define lo siguiente:

- Las zonas, puertas y lectoras de credenciales, la video vigilancia y los sistemas auxiliares de seguridad de las instalaciones
- Los niveles de acceso necesarios por los diversos grupos de personas que trabajan en las instalaciones
- Los horarios de acceso para los días hábiles y feriados
- Las funciones de operador de las personas que vayan a administrar y monitorear goEntry

Este capítulo está organizado de forma secuencial, con las tareas dispuestas en el orden en que deben ejecutarse para configurar el software goEntry.

1. **Actualizar Firmware Controlador del Sistema goEntry**.
2. **Verificar los diagnósticos**.
3. **Configurar la fecha y hora**.
4. **Crear un certificado de seguridad**.
5. **Cargar un certificado de seguridad**.
6. **Habilitar SSL/HTTPS**.
7. **Configurar la seguridad de las instalaciones**.
8. **Agregar un formato de tarjeta**.
9. **Asignar nombres significativos al hardware detectado**.
10. **Configurar goEntry**.
11. Opcional: **Configurar los módulos de expansión de E/S**.
12. **Configurar los controladores de puertas**.
13. **Configurar puertas**.
14. **Configurar las lectoras**.

15. Opcional: **Agregar una DVR**.
16. Opcional: **Añadir una cámara de video**.
17. Opcional: **Enlazar las cámaras a los dispositivos de rastreo de videos de eventos**.
18. Opcional: **Agregar una área**.
19. Opcional: **Configurar el Anti-passback**.
20. Opcional: **Asignar lectoras a las áreas**.
21. Opcional: **Agregar un grupo de feriados**.
22. Opcional: **Agregar un horario**.
23. Opcional: **Agregar un grupo de lectoras**.
24. **Agregar un nivel de acceso**.
25. Opcional: **Agregar un rol de operador**.
26. Opcional: **Añadir campos definidos por usuario**.
27. Opcional: **Comportamiento programación de puertas y lectoras**.
28. **Importar personas y credenciales de un archivo CSV**.
29. **Crear un respaldo y un punto de restauración**.

Actualizar Firmware Controlador del Sistema goEntry

1. Abrir el navegador de Internet.
2. Descargar la última actualización del firmware goEntry.
3. Iniciar sesión en goEntry.
    a. Escribir direcciones IP para goEntry en la barra direcciones del navegador.
    b. Si al usar Internet Explorer recibe una advertencia sobre el certificado de seguridad, seleccionar **Pasar a este sitio web (no recomendado)**.
    c. Escribir **Nombre usuario**.
    d. Escribir **Contraseña**.
    e. Seleccionar **Idioma**.
    f. Hacer clic en [Iniciar sesión].
4. Seleccionar ***Administración del sistema > Actualizaciones firmware***.
5. Hacer clic en [Buscar].
6. Navegar y seleccionar archivo actualización del firmware.
7. Hacer clic en [Actualizar].
8. Verificar los diagnósticos

En la pantalla de diagnóstico de goEntry, comprobar que no hay ningún problema con las puertas, controladores y otros dispositivos recién instalados.

Ver **Diagnóstico en pág. 67.**

Configurar la fecha y hora

goEntry admite la sincronización temporal con un servidor NTP. Esta opción, si está habilitada tanto en goEntry como en la DVR, mantiene la(s) DVR(s) y goEntry sincronizados temporalmente. Caso

contrario, la hora de goEntry puede variar en relación con la hora de la(s) DVR(s) y dificultar o imposibilitar la recuperación del video relacionado con un evento de acceso. El cliente NTP trata de sincronizarse de hora en hora.

Nota: TVR10 no admite la sincronización temporal con un servidor NTP.

Nota: Si la hora de goEntry se cambia manualmente a menos de un minuto antes del comienzo de un horario asignado a una puerta, el modo horario de la puerta surte efecto de inmediato.

1. Seleccionar ***Administración del sistema > Configuración del sistema***.
2. Hacer clic en la etiqueta **Fecha y hora**.
3. Seleccionar la **zona horaria**.
4. Seleccionar la **fecha y hora** local.
5. Opcional: Sincronizar la hora:
   a. Seleccionar [Sincronizar con servidor NTP].
      La sincronización temporal con el servidor NTP requiere el acceso desde el panel al servidor NTP a través del puerto UDP 123. Si este puerto no está accesible, la hora del panel no se sincroniza con el servidor NTP y se registran eventos de "Error de sinc. NTP".
   b. Escribir la dirección IP del servidor NTP.
   c. Hacer clic en [Sincronizar ahora].

Configuración de seguridad de la red

La etiqueta Configuración de red de la página Ajustes del sistema permite asignar un certificado de seguridad y configurar las propiedades de la red, incluida la navegación segura de goEntry.

Crear un certificado de seguridad

1. Seleccionar ***Administración del sistema > Ajustes del sistema***.
2. Hacer clic en la etiqueta **Configuración de red**.
3. Pulsar el botón [Crear una solicitud de firma de certificado].
   Aparece la caja de diálogo Solicitud de firma de certificado.
4. Escribir la información solicitada y hacer clic en [Generar].
   En la caja de texto, en el lado derecho de la caja de diálogo, aparece el texto de la Solicitud de firma de certificado.
5. Para usar un certificado autofirmado:
   a. Hacer clic en [Instalar certificado autofirmado].
   b. Reiniciar el controlador cuando se le solicite.
6. Para usar un certificado firmado:
   a. Copiar el texto de la Solicitud de firma de certificado y guardar en un archivo local para enviarlo a la autoridad de certificación que se prefiera
   b. Cerrar la caja de diálogo Solicitud de firma de certificado.
   c. Ver **Cargar un certificado de seguridad en pág. 14.**

Cargar un certificado de seguridad

1. Seleccionar ***Administración del sistema > Ajustes del sistema***.
2. Hacer clic en la etiqueta **Configuración de red**.
3. Pulsar el botón [Importar certificado]. Aparece la caja de diálogo Cargar certificado.
4. Hacer clic en [Seleccionar archivo].
5. Buscar y seleccionar el archivo del certificado.
6. Hacer clic en [Abrir].
7. Hacer clic en [Cargar].
8. Reiniciar el controlador cuando se le solicite.

Habilitar SSL/HTTPS

IMPORTANTE: No es recomendable operar goEntry sin la seguridad de HTTPS. HTTPS encripta las comunicaciones entre goEntry y el navegador cliente para garantizar que intrusos no puedan interceptar las comunicaciones y acceder al servidor.

1. Seleccionar ***Administración del sistema > Ajustes del sistema***.
2. Hacer clic en la etiqueta **Configuración de red**.
3. Pulsar el botón [Configurar].

   Aparece la hoja de propiedades Propiedades de red.
4. Seleccionar **Habilitar conexión HTTPS**.

Nota: Puede haber casos en los que es necesario usar el protocolo de hipertexto no seguro (HTTP). Por ejemplo, si se accede al controlador del sistema goEntry a través de un servidor de red proxy no compatible con HTTPS (SSL), la única opción es deshabilitar HTTPS/SSL.

Nota: Tras habilitar o deshabilitar HTTPS/SSL, verificar que se limpió la caché del navegador, especialmente si se usa Firefox o Chrome.

Configuración de seguridad

La etiqueta Seguridad de la página Ajustes del sistema permite configurar aspectos relativos a la seguridad física de las instalaciones. La seguridad de la red se configura en la etiqueta Configuración de red.

Códigos PIN

goEntry puede ser configurado para el acceso solo con una credencial o con una credencial y un número de identificación personal (PIN). Exigir que las personas presenten una tarjeta de identificación (credencial) y escriban un código PIN, aumenta la seguridad al impedir el acceso con una tarjeta de identificación encontrada o robada. Las lectoras pueden configurarse para Solo credencial o Credencial y PIN, según los horarios. (Ver **Comportamiento programación de puertas y lectoras en pág. 37.**)

Longitud máxima del PIN

El PIN puede tener 4, 6 ó 9 dígitos.

Intentos de PIN

Permite que las personas intenten introducir su PIN correctamente una cierta cantidad de veces.

Tiempo de bloqueo de PIN

Si una persona entra un PIN incorrecto demasiadas veces, se impide el acceso de la identificación de la credencial a esa lectora durante el tiempo especificado en esta opción. Una vez transcurrido el tiempo de bloqueo, se restauran los privilegios de acceso de la identificación de la credencial.

Modo Puerta degradada

La información de las credenciales se almacena en el controlador del sistema goEntry. Si un controlador de puertas pierde la comunicación con el controlador, no puede verificar las credenciales escaneadas por las lectoras con la base de datos almacenada en el controlador. En tal caso, el controlador de puertas debe validar las solicitudes de acceso si alguien ha de entrar en las instalaciones.

Terminaciones EOL de entrada

Las puertas pueden ser cableadas para detectar si están abiertas o cerradas, forzadas y saboteadas. A estas puertas se las llama supervisadas. A las puertas sin circuitos de detección se las llama no supervisadas, aunque tengan una lectora y una cerradura eléctrica o un bloqueo magnético. Para puertas supervisadas, esta opción describe el tipo de resistencia(s) que se usan y cómo se cablea el circuito. Hay dos tipos principales monitoreados por goEntry: circuitos de 1,000 y de 4,700 ohmios. Pueden cablearse con resistencias dobles o con una sola resistencia conectadas en serie o en paralelo en relación con el sensor de la puerta.

Configurar la seguridad de las instalaciones

1. Seleccionar ***Administración del sistema > Ajustes del sistema***.
2. Hacer clic en la etiqueta **Seguridad**.
3. Seleccionar la **longitud máxima de PIN**.

   IMPORTANTE: Cuando se salva una nueva longitud máxima de PIN y existen credenciales con números de PIN más largos que la nueva longitud máxima, aparece una advertencia diciendo que los números de PIN existentes se truncarán para adaptarlos a la nueva longitud. El mensaje del sistema permite continuar o cancelar la operación de salvar.

4. Seleccionar la cantidad de **intentos de PIN**.
5. Seleccionar un **tiempo de bloqueo de PIN**.
6. Seleccionar un **modo puerta degradada**:
   - **Restringido**: No se autoriza ningún acceso
   - **Código de sitio**: Se autoriza el acceso si la credencial coincide con uno de los formatos definidos en la página Formatos de tarjeta y el código de sitio en la tarjeta coincide con el definido para el formato
   - **Todos**: Se autoriza el acceso si la tarjeta coincide con alguno de los formatos definidos en la página Formatos de tarjeta
7. Seleccionar una opción de **Terminaciones de EOL entrada**.
8. Hacer clic en [Aceptar cambios].

Configuración de los formatos de tarjeta

Las credenciales (tarjetas de identificación) que se usan para el control de acceso electrónico almacenan los datos en diferentes formatos. A fin de leer correctamente los datos, es necesario agregar el formato de tarjeta a la configuración. La identificación de las credenciales almacenada en la tarjeta incluye un número de tarjeta, un código de las instalaciones y un código de emisión.

Agregar un formato de tarjeta

1. Seleccionar ***Administración del sistema > Formatos de tarjeta***.
2. Hacer clic en [Añadir].
3. Escribir un nombre descriptivo en el campo **Nombre del formato**.
4. Seleccionar un **tipo de formato**.
5. Tipo de **código de instalación**, si es necesario.
6. Para un formato personalizado, escribir otros datos, según sea necesario.
7. Hacer clic en [Aceptar cambios].

Eliminar un Formato de tarjeta

1. Seleccionar ***Administración del sistema > Formatos de tarjeta***.
2. Seleccionar el formato de tarjeta a eliminar.
3. Hacer clic en [Remover].

   Aparece caja de diálogo Remover item.
4. Hacer clic en [Remover].

Formatos de tarjeta por default

goEntry tiene los siguientes formatos de credenciales instalados por default:

- 4002 40 bits (40 bits CASI 4002)
- En bruto 32 bits (32 bits 14443 Cascade 1)
- Wiegand 26 bits (26 bits Wiegand)

Estos formatos pueden eliminarse, si es necesario agregar otros. goEntry admite hasta ocho formatos de tarjeta activos.

Configuración de dispositivos

Una vez instalado y conectado el hardware, el controlador del sistema goEntry detecta automáticamente todos los dispositivos instalados y los presenta en una jerarquía de árbol en la página Dispositivos. goEntry asigna nombres genéricos, secuenciales, a los dispositivos que detecta. Estos nombres deben reemplazarse con nombres significativos, para facilitar el monitoreo de eventos de acceso. Por ejemplo, "Controlador de puertas (3)" puede cambiarse por "Vestíbulo principal, puertas en la pared Este". Para cambiar el nombre de los dispositivos de esta manera, es necesario un registro del número de serie de cada dispositivo y el lugar en que están instalados.

La configuración de los dispositivos implica más que el mero cambio de nombres. En esta página también se configuran entradas y salidas opcionales, temporizadores de alarma, monitoreo por video y temporizadores ampliados para el acceso de personas con discapacidad.

Nota: Para conectarse a una cámara de video o DVR, véase Configuración de dispositivos de video en pág. 25.

Asignar nombres significativos al hardware detectado

Para sistemas con más de unos pocos dispositivos, es recomendable ejecutar esta tarea para todos los dispositivos antes de proceder con la configuración detallada de los dispositivos, a fin de no perder de vista la ubicación física de los dispositivos, a medida que se avanza con los requisitos detallados.

Antes de comenzar esta tarea, obtener la tabla de configuración de las instalaciones, que muestra la ubicación física de cada dispositivo.

1. Seleccionar ***Administración del sistema > Dispositivos***.
2. Seleccionar el controlador del sistema goEntry.
3. Escribir un **Nombre del dispositivo** descriptivo.
4. Hacer clic en [Aceptar cambios].
5. Seleccionar el primer controlador de puertas de la lista.
6. Comparar el **número de serie** con la tabla de instalación.
7. Escribir un **Nombre del dispositivo** descriptivo.
8. Hacer clic en [Aceptar cambios].
9. Repetir este procedimiento para cada uno de los dispositivos en la jerarquía.

Configurar goEntry

goEntry puede aceptar cuatro entradas auxiliares de uso general y emitir dos señales de uso general, que deben activarse manualmente. Las entradas se pueden usar para accesorios tales como un detector de movimiento o para entradas de otros sistemas como, por ejemplo, un sistema de alarma de incendio. Se trata de configuraciones opcionales y solo deben habilitarse si están instaladas. Las entradas de uso general pueden configurarse para abrir todas las puertas automáticamente al ser disparadas, como en el caso de una alarma de incendio u otra emergencia.

1. Seleccionar ***Administración del sistema > Dispositivos***.
2. Seleccionar el controlador del sistema goEntry.
3. Hacer clic en la etiqueta **General**.
4. Seleccionar una **cámara enlazada**, si se ha configurado una para monitorear la ubicación física del controlador.
5. Hacer clic en la etiqueta **Entradas**.
6. Para cada entrada auxiliar de uso general que se conecta:
   a. Seleccionar **Habilitado**.
   b. Escribir un nombre significativo.
   c. Seleccionar el **Tipo**.
   d. Opcional: Seleccionar **Desbloquear todas las puertas**, si la entrada es de un sistema de alarma o emergencia.
   e. Opcional: Seleccionar una **cámara enlazada**, si hay una asociada a la fuente de entrada (por ejemplo, una cámara asociada a un detector de movimiento).

7. Hacer clic en la etiqueta **Salidas**.
8. Para cada salida auxiliar de uso general que se conecta:
   a. Seleccionar **Habilitado**.
   b. Escribir un nombre significativo.
   c. Seleccionar **Activado/desactivado**, si el relé se energiza cuando la salida es activada, de lo contrario, no marcar la caja de selección.
   d. Opcional: Seleccionar una **cámara enlazada**, si hay una asociada a la salida.
9. Hacer clic en [Aceptar cambios].

goEntry Entradas y Salidas

Las entradas y salidas son opciones generales que permiten personalizar goEntry a las necesidades de la organización. Una entrada puede ser la señal de un detector de movimiento, por ejemplo. Una salida es un impulso eléctrico enviado por el controlador goEntry a algún dispositivo. Las entradas y salidas se monitorean desde la página ***Monitoreo > Entradas/salidas***, desde donde se pueden activar manualmente las salidas.

Configurar los controladores de puertas

Los controladores de puertas se pueden conectar a un máximo de cuatro lectoras en dos puertas. Cada puerta puede tener dos lectoras, una para entrar y una para salir, usadas usualmente con Anti-passback.

1. Seleccionar ***Administración del sistema > Dispositivos***.
2. Expandir el árbol bajo controlador del sistema goEntry.
3. Seleccionar el Controlador de puertas.
4. Seleccionar la **Cantidad de puertas** conectadas a este controlador.
5. Opcional: Seleccionar una **cámara enlazada**, si hay una asociada al panel del controlador de puertas.
6. Hacer clic en [Aceptar cambios].

Nota: Aunque todas las puertas estén bloqueadas al agregar un nuevo controlador de puerta, éste permanecerá desbloqueado. Para bloquearlo, se deben restablecer todas las puertas para bloquearlas a todas nuevamente.

Configuración de las puertas

Para cada puerta deben configurarse los siguientes parámetros:

- período de tiempo que debe permanecer desbloqueada cuando se presenta una credencial válida
- período de tiempo que se la puede mantener abierta antes de disparar una alarma
- el tipo de cerradura usada (ya sea eléctrica estándar o con bloqueo magnético)
- si se requiere una lectora solo para entrar o para entrar y salir
- los tipos de eventos y alarmas monitoreados por los circuitos de la puerta
- entradas y relés auxiliares, por ejemplo, una puerta configurada con apertura automática y solicitud de de salida (RTE) ampliada, para facilitar el acceso de discapacitados.

Configurar puertas

1. Abrir el navegador de Internet.

2. Descargar la última actualización del firmware goEntry.
3. Iniciar sesión en goEntry.
   a. Escribir direcciones IP para goEntry en la barra direcciones del navegador.
   b. Si al usar Internet Explorer recibe una advertencia sobre el certificado de seguridad, seleccionar **Pasar a este sitio web (no recomendado)**.
   c. Escribir **Nombre usuario**.
   d. Escribir **Contraseña**.
   e. Seleccionar **Idioma**.
   f. Hacer clic en [Iniciar sesión].
4. Seleccionar ***Administración del sistema > Actualizaciones firmware***.
5. Hacer clic en [Buscar].
6. Navegar y seleccionar archivo actualización del firmware.
7. Hacer clic en [Actualizar].
8. Opcional: seleccionar una **Ampliación del período de acceso autorizado**.
9. Seleccionar el **Tiempo de puerta mantenida abierta**.
10. Opcional: seleccionar una **Extensión del tiempo de puerta mantenida abierta**.
11. Seleccionar un **Modo de cerradura**
    - **Desbloqueo programado**
    - **Bloquear al cerrar**
12. Opcional: seleccionar una **cámara enlazada**, si hay una posicionada para monitorear la puerta.
13. Seleccionar un **Modo de acceso**.
14. Opcional: Seleccionar **Solicitud de salida habilitada**, si la puerta está cableada al efecto.
15. Opcional: Seleccionar las alarmas conectadas a la puerta:
    - **Puerta mantenida abierta**
    - **Puerta Forzada Abierta**
    - **Sabotaje**
16. Opcional: Si se ha conectado una alarma visual o auditiva a la puerta, seleccionar "Puerta Mantenida/forzada" en la lista de **Relés auxiliares**.
17. Configurar los **Tipos de entrada** de los sensores:
    - Sensor de **contacto de la puerta**
    - Botón o sensor de **Solicitud de salida**
    - Entrada **auxiliar** de la solicitud de salida extendida o del sensor de contacto del bloqueo magnético
    - Circuitos **antisabotaje**
18. Hacer clic en [Aceptar cambios].
19. Repetir este procedimiento para cada puerta.

Configurar una puerta para el Acceso de discapacitados

goEntry registra eventos cada vez que las puertas se mantienen abiertas durante demasiado tiempo y cuando se autoriza el acceso, pero la puerta no se abre. Con una alarma visual o auditiva opcional, goEntry puede disparar una alarma física si se forza la puerta o se la mantiene abierta durante demasiado tiempo.

Para adaptarse a las necesidades de las personas que necesitan más tiempo para abrir o pasar a través de una puerta, goEntry permite identificar las credenciales autorizadas al efecto y configurar

características opcionales en una puerta, tales como apertura automática y tiempo extra para los sensores de solicitud de salida. Esto se realiza de credencial en credencial, para preservar la seguridad de las instalaciones, puesto que cuanto más tiempo una puerta se mantiene abierta, más fácil es que alguien entre sin presentar una credencial. Ver **Añadir una credencial en pág. 41.**

1. Abrir el navegador de Internet.
2. Descargar la última actualización del firmware goEntry.
3. Iniciar sesión en goEntry.
    a. Escribir direcciones IP para goEntry en la barra direcciones del navegador.
    b. Si al usar Internet Explorer recibe una advertencia sobre el certificado de seguridad, seleccionar **Pasar a este sitio web (no recomendado)**.
    c. Escribir **Nombre usuario**.
    d. Escribir **Contraseña**.
    e. Seleccionar **Idioma**.
    f. Hacer clic en [Iniciar sesión].
4. Seleccionar ***Administración del sistema > Actualizaciones firmware***.
5. Hacer clic en [Buscar].
6. Navegar y seleccionar archivo actualización del firmware.
7. Hacer clic en [Actualizar].
8. Seleccionar una **Extensión del período de acceso autorizado**.

    Este es el período de tiempo que la puerta permanece desbloqueada para que la persona la pueda abrir.
9. Seleccionar el **Tiempo de puerta mantenida abierta**.
10. Seleccionar una **Extensión del tiempo de puerta mantenida abierta**.

    Este es el período de tiempo que la puerta puede permanecer abierta para que la persona la atraviese.
11. Seleccionar un **Modo de cerradura**
    - **Desbloqueo programado**
    - **Bloquear al cerrar**
12. Opcional: seleccionar una **cámara enlazada**, si hay una posicionada para monitorear la puerta.
13. Seleccionar un **Modo de acceso**.
14. Opcional: seleccionar **Solicitud de salida habilitada**, si la puerta está cableada al efecto.
15. Opcional: seleccionar las alarmas conectadas a la puerta:
    - **Puerta mantenida abierta**
    - **Puerta Forzada Abierta**
    - **Sabotaje**
16. Si la puerta está conectada a un dispositivo de apertura automática:
    a. Seleccionar "RTE Extendido" en la lista de **Entradas auxiliares**.
    b. Seleccionar "**Apertura automática**" en la lista de **Entradas auxiliares**.
    c. Seleccionar un **Tiempo de activación del relé auxiliar**.
17. Configurar los **Tipos de entrada** de los sensores:
    - Sensor de **contacto de la puerta**
    - Botón o sensor de **Solicitud de salida**
    - Entrada **auxiliar** de la solicitud de salida extendida o del sensor de contacto del bloqueo magnético
    - Circuitos **antisabotaje**

18. Hacer clic en [Aceptar cambios].
19. Repetir este procedimiento para cada puerta.

Configurar una puerta con bloqueo magnético

• *ADVERTENCIA* • Al configurar una puerta con bloqueo magnético, es importante usar la opción "Sensor de conexión del bloqueo magnético" para evitar que los imanes de la puerta se activen antes de tiempo y cierren la puerta de golpe, lo que puede causar lesiones.

1. Abrir el navegador de Internet.
2. Descargar la última actualización del firmware goEntry.
3. Iniciar sesión en goEntry.
   a. Escribir direcciones IP para goEntry en la barra direcciones del navegador.
   b. Si al usar Internet Explorer recibe una advertencia sobre el certificado de seguridad, seleccionar **Pasar a este sitio web (no recomendado)**.
   c. Escribir **Nombre usuario**.
   d. Escribir **Contraseña**.
   e. Seleccionar **Idioma**.
   f. Hacer clic en [Iniciar sesión].
4. Seleccionar ***Administración del sistema > Actualizaciones firmware***.
5. Hacer clic en [Buscar].
6. Navegar y seleccionar archivo actualización del firmware.
7. Hacer clic en [Actualizar].
8. Opcional: seleccionar una **Ampliación del período de acceso autorizado**.
9. Seleccionar el **Tiempo de puerta mantenida abierta**.
10. Opcional: seleccionar una **Extensión del tiempo de puerta mantenida abierta**.
11. Seleccionar un **Modo de cerradura**:
    - **Desbloqueo programado**
    - **Bloquear al cerrar**
12. Opcional: seleccionar una **cámara enlazada**, si hay una posicionada para monitorear la puerta.
13. Seleccionar un **Modo de acceso**.
14. Opcional: Seleccionar **Solicitud de salida habilitada**, si la puerta está cableada al efecto.
15. Opcional: Seleccionar las alarmas conectadas a la puerta:
    - **Puerta mantenida abierta**
    - **Puerta Forzada Abierta**
    - **Sabotaje**
16. Seleccionar "**Sensor de conexión del bloqueo magnético**" en la lista de **Entradas auxiliares**.
17. Opcional: Si se ha conectado una alarma visual o auditiva a la puerta, seleccionar "Puerta mantenida/forzada" en la lista de **Relés auxiliares** .
18. Configurar los **Tipos de entrada** de los sensores:
    - Sensor de **contacto de la puerta**
    - Botón o sensor de **Solicitud de salida**
    - Entrada **auxiliar** de la solicitud de salida extendida o del sensor de contacto del bloqueo magnético
    - Circuitos **antisabotaje**

19. Hacer clic en [Aceptar cambios].
20. Repetir este procedimiento para cada puerta.

Opciones de configuración de puertas

Período Normal de Acceso Autorizado

Cuando una lectora escanea una credencial válida, la puerta se desbloquea durante el tiempo seleccionado.

Ampliación del período de acceso autorizado

Cuando una lectora escanea una credencial válida con la opción **tiempo mantenida abierta/ extendida** seleccionada, la puerta se desbloquea durante este periodo de tiempo. Esto permite configurar el sistema de modo de cumplir la legislación y los reglamentos que rigen el acceso de personas con discapacidad.

Ver **Añadir una credencial en pág. 41.**

Tiempo de puerta mantenida abierta

Cuando la lectora escanea una credencial válida, la puerta puede mantenerse abierta durante este período de tiempo. Si una puerta se mantiene abierta durante más tiempo que el especificado, se registra un evento y se selecciona la opción **Puerta mantenida abierta**.

Tiempo ampliado de puerta mantenida abierta

Cuando una lectora escanea una credencial válida con la opción **tiempo extendido de mantenida/abierta** seleccionada, la puerta puede mantenerse abierta durante este periodo de tiempo. Si una puerta se mantiene abierta durante más tiempo que el especificado, se registra un evento y se selecciona la opción **Puerta mantenida abierta**. Esto permite configurar el sistema de modo de cumplir la legislación y los reglamentos que rigen el acceso de personas con discapacidad.

Ver **Añadir una credencial en pág. 41.**

Solicitud de salida habilitada

Si la puerta cuenta con alarma por violación, mantenida abierta demasiado tiempo y sabotaje, se debe usar Solicitud de salida, conjuntamente con un botón que se presiona para salir, una lectora de salida o algún tipo de sensor que detecta la aproximación a la puerta desde el interior. De lo contrario, cada vez que alguien sale, se dispara una alarma de puerta forzada.

Modo de cerradura

Desbloqueo programado

La puerta se desbloquea cuando se autoriza el acceso y permanece desbloqueada hasta que expira el período especificado en **Período normal de acceso autorizado**.

Si la **entrada auxiliar** de la puerta está configurada con Sensor de conexión del bloqueo magnético, el relé de apertura permanece activo hasta que se activa el sensor de conexión magnética, se cierra el contacto de la puerta y expira el tiempo de desbloqueo.

Bloquear al cerrar

La puerta se desbloquea cuando se autoriza el acceso y permanece desbloqueada hasta que expira el período especificado en **Período normal de acceso autorizado** o se abre y cierra la puerta, lo que tenga lugar primero.

Si la **entrada auxiliar** de la puerta está configurada con Sensor de conexión del bloqueo magnético, el relé de apertura permanece activo hasta que se activa el sensor de conexión magnética y se cierra el contacto de la puerta, independientemente del tiempo de desbloqueo.

Modo de acceso

Lectora solo para entrar

La puerta tiene una lectora para escanear credenciales para entrar, pero no requiere la presentación de credenciales para salir.

Lectora para entrar y lectora para salir

La puerta tiene lectoras para escanear credenciales para entrar y para salir. Esta configuración es necesaria para la función Anti-passback.

Alarma habilitada

Puerta mantenida abierta

Seleccionar esta opción si la puerta está cableada de modo de detectar que está abierta. Si se mantiene abierta durante más tiempo que el seleccionado en **Tiempo de puerta mantenida abierta**, se registra un evento en la página Eventos.

Puerta Forzada Abierta

Seleccionar esta opción si la puerta está cableada para detectar una entrada forzada. Si una persona abre la puerta, sin presentar una credencial con acceso autorizado, se registra un evento en la página Eventos. Si se desea que se dispare una alarma física cuando la puerta es forzada, configurarla con una alarma visual o auditiva cableada al **relé auxiliar**.

Sabotaje

Seleccionar esta opción si la puerta está cableada para detectar sabotaje. En caso de sabotaje, se registra un evento en la Página Eventos.

Entrada auxiliar

Ninguno

Indica que la entrada no se usa ni se monitorea.

Solicitud de salida ampliada

Concebida para uso únicamente con la opción Apertura automática seleccionada en **Relés auxiliares**.

Sensor de conexión del bloqueo magnético

Concebido para puertas con bloqueo magnético en vez de cerradura eléctrica estándar. Detecta la señal de salida del bloqueo magnético que indica que la puerta se ha conectado con el imán. goEntry no activa el imán hasta que el sensor de conexión de la puerta envía una señal que indica que la puerta se conectó con el imán y el sensor de contacto de la puerta indica que la puerta está cerrada. De este modo se evita que el imán se active antes de tiempo y la puerta se cierre de golpe.

Si "Desbloqueo programado" es el **Modo de cerradura de puerta** seleccionado, el imán permanece inactivo hasta que expira el período determinado. De cualquier modo, no se activa hasta que se reciben las señales del sensor de conexión magnética y del sensor de contacto de la puerta, indicando que la puerta está cerrada y conectada al imán.

Relé auxiliar

Ninguno

Indica que el relé no se usa ni se energiza.

Puerta mantenida/forzada
Un uso típico de esta opción es hacer que el relé dispare una alarma física, visual o auditiva, cuando se sujeta o se viola la puerta.

Abridor puerta
Por lo general, se usa con una puerta configurada con una sola lectora de entrada y un dispositivo manual de liberación cableado como Solicitud de salida (RTE) y un pulsador para apertura automática de RTE extendida. La entrada de RTE abre la puerta durante el tiempo que el dispositivo manual de liberación está activo, suficiente para que una persona salga con normalidad. La entrada auxiliar (RTE extendida) activa el relé auxiliar durante el Tiempo especificado de activación del relé auxiliar. Esta salida de relé activa el dispositivo de apertura automática de la puerta, que la desbloquea y la abre para dejar pasar a una persona con necesidades especiales.

Esta configuración solo tiene sentido si la **entrada auxiliar** está configurada para RTE extendida.

Tipos de entrada

NA (normalmente abierto)
El contacto del sensor está normalmente abierto.

NC (normalmente cerrado)
El contacto del sensor está normalmente cerrado.

No supervisada
El circuito no está cableado con un circuito de continuidad para detectar sabotaje.

Supervisada
El circuito está cableado con un circuito de continuidad para detectar sabotaje.

Configurar las lectoras

1. Seleccionar ***Administración del sistema > Dispositivos***.
2. Expandir el árbol bajo controlador del sistema goEntry.
3. Expandir el árbol bajo controlador de puertas.
4. Expandir el árbol debajo de la puerta.
5. Seleccionar la lectora a configurar.
6. Seleccionar un **Método de acceso**.
   - **Solo credencial**
   - **Credencial y PIN**
7. Seleccionar una **cámara enlazada**, si hay una posicionada para monitorear la puerta y la lectora.
8. Hacer clic en [Aceptar cambios].
9. Repetir este procedimiento para las otras lectoras.

Opciones de lectoras

Solo Credencial
Para accesar, solo es necesario presentar una credencial válida (ID de Credencial).

Credencial y PIN
Para accesar, es necesario presentar una credencial válida y un número de identificación personal. Esto impide el acceso con una credencial robada o encontrada. Algunas instalaciones usan el

modo **Solo credencial** durante el día y **Credencial y PIN** fuera del horario laboral, cuando las instalaciones están vacías.

Configurar los módulos de expansión de E/S

1. Seleccionar ***Administración del sistema > Dispositivos***.
2. Seleccionar expansor de E/S.
3. Hacer clic en la etiqueta **General**.
4. Seleccionar una **cámara enlazada**, si se ha configurado una para monitorear la ubicación física del controlador.
5. Seleccionar **Alarma de sabotaje habilitada**, si el gabinete está diseñado para detectar sabotajes.
6. Hacer clic en la etiqueta **Entradas**.
7. Para cada entrada auxiliar de uso general que se conecta:
    a. Seleccionar **Habilitado**.
    b. Escribir un nombre significativo.
    c. Seleccionar el **Tipo**.
    d. Opcional: Seleccionar **Desbloquear todas las puertas**, si la entrada es de un sistema de alarma o emergencia.
    e. Opcional: Seleccionar una **cámara enlazada**, si hay una asociada a la fuente de entrada (por ejemplo, una cámara asociada a un detector de movimiento).
8. Para cada salida auxiliar de uso general que se conecta:
    a. Seleccionar **Habilitado**.
    b. Escribir un nombre significativo.
    c. Seleccionar **Activado/desactivado**, si el relé se energiza cuando la salida es activada, de lo contrario, no marcar la caja de selección.
    d. Opcional: Seleccionar una **cámara enlazada**, si hay una asociada a la salida.
9. Hacer clic en [Aceptar cambios].

Configuración de dispositivos de video

goEntry permite revisar los registros de video de los eventos de acceso, mediante el acceso a videos grabados en TVR10 o TVR30/TVR31 a través de las cámaras asociadas a los dispositivos conectados al controlador del sistema goEntry. Cuando se produce un evento en un dispositivo, goEntry mantiene un registro de la fecha y hora del evento. Si hay una cámara vinculada a ese dispositivo, goEntry usa la fecha y hora del evento para crear un hipervínculo a un video grabado por la DVR conectada a la cámara.

Nota: TVR10 está disponible en los Estados Unidos y Europa, TVR30/TVR31 está disponible solo en los Estados Unidos.

Enlazar una cámara a un dispositivo permite que goEntry asocie un evento producido en tal dispositivo al video grabado a través de la cámara durante el tiempo del evento. goEntry no controla la cámara ni la DVR directamente, sino que usa la información para transmitir a la DVR la fecha y hora y la cámara que grabó el video, para reproducirlo.

Las cámaras de video de vigilancia pueden ser de dos tipos generales: fija o con movimiento horizontal, vertical y zoom (PTZ). goEntry permite controlar las cámaras PTZ, si:

- Está usando el navegador Internet Explorer
- ActiveX y .NET 4.0 están instalados o habilitados en el navegador
- La cámara está conectada a una TVR10 o TVR30/TVR31

Agregar una DVR

goEntry se puede conectar a las DVRs TVR10 y TVR30/TVR31 marca UTC Fire and Security. Para trabajar con goEntry, deben estar a los siguientes niveles de firmware:

- TVR30: 0617-0380-0625-6300 (o posterior)
- TVR31: 031F-028A-0676-8000 (o posterior)
- TVR10: v2.3 compilación 100916 (o posterior)

Consultar la documentación de TVR para obtener instrucciones para verificar y actualizar las versiones de firmware.

1. Seleccionar ***Administración del sistema > Dispositivos > Dispositivos de video***.
2. Hacer clic en [Agregar] y seleccionar el modelo adecuado de DVR.
3. Escribir un nombre descriptivo en el campo **Nombre del dispositivo**.
4. Escribir la **dirección IP** de la DVR.
5. Escribir el **nombre de usuario** para iniciar sesión en el dispositivo.
6. Escribir la contraseña para iniciar sesión en el dispositivo.
7. Hacer clic en [Aceptar cambios].
8. Hacer clic en el siguiente enlace **Configuración y control del navegador web** para confirmar la conexión y comprobar la configuración de las cámaras conectadas a la DVR.

Añadir una cámara de video

Antes de ejecutar esta tarea, se debe añadir un dispositivo TVR10 o TVR30/TVR31 a goEntry.

Nota: TVR10 está disponible en los Estados Unidos y Europa, TVR30/TVR31 está disponible solo en los Estados Unidos.

1. Select ***Administración de Sistema > Dispositivos > Dispositivos de Video***.
2. Seleccionar la DVR con la cámara por añadir.
3. Seleccionar ***Añadir > cámara***.
4. Escribir un nombre descriptivo en el campo **Nombre del dispositivo**.

   Por ejemplo, "Cámara del vestíbulo principal".
5. Seleccionar la **Entrada de DVR** correcta.

   Es el canal en la DVR al que se conecta físicamente la cámara.
6. Seleccionar un **Ancho de banda del flujo de video**.

   En caso de duda sobre el ancho de banda, iniciar sesión en la interfaz web de la DVR y consultar la configuración de la cámara.
7. Escribir la **Duración de la reproducción previa al evento** deseada.

   Es la cantidad de tiempo previo al evento que desea ver en la reproducción. Por ejemplo, una evento de puerta forzada se registra en el sistema cuando la puerta se forza, sin embargo, la

persona que forzó la puerta puede haberla saboteado durante varios segundos antes de lograr forzarla.

Agregar plantillas de video

Las plantillas de video determinan cuántas entradas de cámara se pueden monitorear simultáneamente desde la pantalla de la computadora.

1. Seleccionar ***Monitoreo > Plantillas de video***.
2. Hacer clic en [Añadir].
3. Escribir un nombre descriptivo en el campo **Nombre de la plantilla de video**.

   Por ejemplo, si hay cuatro cámaras vigilando la zona de la plataforma de carga, es posible crear una plantilla 2x2 y llamarla "Cámaras de la plataforma de carga".
4. Seleccionar un **Tipo de plantilla de video**.
5. Seleccionar una cámara para cada celda de la plantilla.
6. Hacer clic en [Aceptar cambios].

Enlazar las cámaras a los dispositivos de rastreo de videos de eventos

Las lectoras generan eventos de acceso autorizado y acceso denegado, por lo que, si se enlaza una cámara a una lectora, se tiene un registro visual de cada persona que entró (o a la cual se le denegó la entrada) por esa lectora.

Las puertas generan eventos si se las forza, se las mantiene abiertas durante demasiado tiempo y en caso de desbloqueo momentáneo, por lo que, si se enlaza una cámara a una puerta, se tiene un registro de cada incidente de seguridad de acceso.

Entradas y salidas auxiliares son dispositivos opcionales conectados al controlador del sistema goEntry o a un módulo de expansión de E/S goEntry. Para enlazar una cámara a estos dispositivos, se debe hacerlo a través de la etiqueta Entrada o Salida del controlador correspondiente.

1. Conectar goEntry (a través de la red TCP/IP) a la DVR y la cámara.
   a. Ver **Agregar una DVR en pág. 26.**
   b. Ver **Añadir una cámara de video en pág. 26.**
2. Seleccionar ***Administración del sistema > Dispositivos***.
3. Seleccionar el dispositivo en el árbol de la página Dispositivos
4. Seleccionar la cámara adecuada en la lista **cámara enlazada**.

Configuración de Áreas

Las áreas representan espacios en el plano físico de las instalaciones, específicamente las entradas y salidas a esos espacios. La definición de áreas permite identificar cuáles lectoras conducen al interior de esos espacios y cuáles lectoras conducen al exterior de esos espacios y al interior de las áreas adyacentes. Las áreas se usan para rastrear la ubicación física de las personas en las instalaciones, lo que puede verse en el Informe de nómina, y para rastrear el Anti-passback de las credenciales.

Agregar una área

Antes de poder asignar lectoras a una área, es necesario crear el área.

1. Seleccionar ***Administración de acceso > Áreas > Definición de áreas***.
2. Hacer clic en [Añadir].
3. Escribir un nombre descriptivo en el campo **Nombre del área**.
4. Seleccionar una opción **Reajuste automático anti-passback**.

   Si se selecciona "Nunca", será necesario restablecer manualmente cada infracción de APB.
5. Hacer clic en [Aceptar cambios].

Asignar lectoras a las áreas

La asignación de lectoras a las áreas es lo que define las áreas en goEntry. goEntry registra qué lectora escanea una credencial y, sobre la base de la asignación de áreas, señala el área en que la persona con esa credencial debe estar y por cuáles lectoras debe pasar antes de trasladarse a otra área.

IMPORTANTE: Comprobar la correcta asignación de las lectoras. Si goEntry detecta una credencial en una lectora que no es contigua a la última, se dispara una violación de Anti-passback. Por ejemplo, si el laboratorio A da al pasillo principal y está físicamente configurado de modo que la lectora 1 autoriza el acceso y la lectora 2, la salida, pero, por error, se asignó la lectora 3 para salida, cada persona que intente salir del laboratorio A infringirá el Anti-passback.

1. Seleccionar ***Administración de acceso > Áreas > Asignación de lectoras***.
2. Para cada lectora:
   a. Seleccionar el **Área de partida**. Esta es el área en la que se encuentra la lectora.
   b. Seleccionar la **Área de llegada**. Esta es el área en la que la persona va a entrar, una vez que la lectora acepte su credencial.
   c. Seleccionar **Anti-passback**:
      - **Ninguno**
      - **Tolerante**
      - **Riguroso**
3. Hacer clic en [Aceptar cambios].

Eliminar una Área

Nota: No se puede eliminar el área por default.

1. Seleccionar ***Administración de acceso > Áreas > Definición de áreas***.
2. Seleccionar área por remover.
3. Hacer clic en [Remover].

   Aparece caja de diálogo Remover item.
4. Hacer clic en [Remover].

Configurar Anti-passback

La opción Anti-passback requiere el uso de una credencial para entrar *y salir* de una área. De esta forma, goEntry rastrea en qué área se encuentra el portador de la credencial, mantiene un registro de los movimientos del personal en áreas protegidas e impide el paso a las áreas lógicamente imposibles.

Si una persona usa una credencial para entrar en una área configurada como Anti-passback y, luego, sale sin usar la credencial (a través de una puerta mantenida abierta por otra persona, por ejemplo), el controlador goEntry no sabe que la persona ha salido de esa área específica. Como resultado, si goEntry está configurado para imponer con rigor el Anti-passback, impide que esa credencial se use para entrar en otra área, incluida la que se acabó de dejar, hasta que la ubicación de la credencial se restablece a una área neutra o predeterminada.

Opciones de anti-passback

Una infracción de Anti-passback tiene lugar cuando una persona presenta una credencial (tarjeta de identificación) para entrar en una área, pero de algún modo sale de la área sin presentar la identificación. El evento se dispara cuando la persona trata de entrar en otra área, no conectada físicamente a la última área en la que se sabe que estuvo.

Ninguno
No se usa la función Anti-passback.

Tolerante
Se registra un evento cuando una credencial infringe el Anti-passback.

Riguroso
La credencial que infringe el Anti-passback no puede acceder a ninguna área, hasta que la ubicación de la credencial se restablece a una área neutra o por defalt.

Configurar el Anti-passback

Para configurar el Anti-passback, hay que agregar a goEntry áreas que coinciden con las áreas de las instalaciones, asignar las lectoras a esas áreas y agregar credenciales a goEntry.

1. Ver **Agregar una área en pág. 28.**
2. Ver **Asignar lectoras a las áreas en pág. 28.**
3. Ver **Añadir una credencial en pág. 41.**

Nota: El panel Credenciales de la página Personas (***Administración de acceso > Personas***) permite exceptuar de los requisitos de Anti-passback a credenciales individuales.

Creación de grupos de feriados

Los feriados son excepciones en los horarios del lugar de trabajo. La creación de un grupo de estos días dará lugar a que goEntry anule el horario normal durante esos días. Si no se desea que un feriado anule un determinado horario, entonces es necesario incluir el grupo de feriados en ese horario.

Por ejemplo, las instalaciones pueden abrir de lunes a viernes a excepción de ciertos feriados anuales, cuando solo el personal de limpieza y los administradores de red deben tener acceso a las instalaciones. El personal de limpieza puede hacer una limpieza a fondo cuando las instalaciones

están cerradas para las actividades normales. Los administradores de red pueden usar los feriados para hacer servicios de mantenimiento y actualización que causarían trastornos en un día normal de trabajo. Para adaptarse a estas necesidades, crear un grupo de feriados para esos días en los que el personal regular no trabaja. Es decir, hay que crear dos horarios y dos niveles de acceso, uno para el personal de oficina y otro para el personal de apoyo (personal de limpieza y administradores de red). Incluir el grupo de feriados en el horario del personal de apoyo, pero no en el horario del personal de oficina. Al configurar el nivel de acceso del personal de apoyo, asignar el horario del personal de apoyo a las lectoras y los grupos de lectoras que el personal de apoyo va a usar. Al configurar el nivel de acceso del personal de oficina, asignar el horario del personal de oficina a las lectoras y los grupos de lectoras que el personal de oficina va a usar.

Agregar un grupo de feriados

1. Seleccionar ***Administración de acceso > Feriados***.
2. Hacer clic en [Añadir].
3. Escribir un nombre descriptivo en el campo **Nombre del grupo de feriados**.

   Por default, un grupo nuevo de feriados contiene un feriado.

   a. Eligir la fecha y el patrón del feriado:
      - **Único**: un evento que se produce una sola vez.
      - **Se repite todos los años**: un evento que ocurre en la misma fecha todos años, tal como el 25 de diciembre.
      - **Personalizado**: un evento que se repite anualmente en un patrón específico, como el Viernes Santo.
4. Para agregar un feriado al grupo, hacer clic en [Agregar] en el panel Lista de feriados y repetir el paso a.
5. Hacer clic en [Aceptar cambios].

Agregar un feriado a un grupo de feriados

1. Seleccionar ***Administración de acceso > Feriados***.
2. Seleccionar el grupo de feriados a modificar en la lista de grupos de feriados.
3. Agregar un feriado al grupo:

   a. Hacer clic en [Agregar] en el panel Lista de feriados.

   b. Eligir la fecha y el patrón del feriado:
      - **Único**: un evento que se produce una sola vez.
      - **Se repite todos los años**: un evento que ocurre en la misma fecha todos años, tal como el 25 de diciembre.
      - **Personalizado**: un evento que se repite anualmente en un patrón específico, como el Viernes Santo.
4. Hacer clic en [Aceptar cambios].

grupo de feriados

1. Seleccionar ***Administración de acceso > Feriados***.
2. Seleccionar el grupo de feriados a copiar en la lista de grupos de feriados.
3. Hacer clic en [Copiar].
4. Escribir un nombre descriptivo en el campo **Nombre del grupo de feriados**.
5. Hacer los cambios necesarios en los feriados en el grupo copiado.

6. Hacer clic en [Aceptar cambios].

Eliminar un grupo de feriados

NOTA: No se puede eliminar un grupo de feriados en uso.

1. Seleccionar ***Administración de acceso > Feriados***.
2. Seleccionar el grupo de feriados a eliminar en la lista de grupos de feriados.
3. Hacer clic en [Remover].

   Aparece caja de diálogo Remover item.
4. Hacer clic en [Remover].

Creación de horarios

Los horarios se usan para determinar cuándo una lectora le autorizará el acceso a una persona, o cuándo una puerta se bloquea o desbloquea automáticamente. Los horarios para controlar los períodos de acceso de las lectoras se asignan a través de la página ***Administración de acceso > Niveles de acceso***. Los horarios para controlar el bloqueo de las puertas se asignan a través de la página ***Monitoreo > Puertas***.

goEntry permite crear hasta 64 horarios e incluye los siguientes horarios predeterminados:

- Todos los días las 24 horas del día
- Lunes a viernes 8AM-5PM (8.00 a 17.00)
- Lunes a viernes 9AM-6PM (9.00 a 18.00)
- Fines de semana 7AM-7PM (7.00 a 19.00)

Nota: En los horarios, el tiempo se expresa en horas y minutos, sin segundos, pero la hora de inicio de un período corresponde al comienzo del minuto (0 segundos) y la hora de término de un período corresponde al final del minuto (59 segundos). Al observar el horario predefinido de todos los días de la semana las 24 hora del día, se nota que la hora de inicio es 12:00 AM (24.00) y la hora de término es 11:59 PM (23.59). Expresado en segundos, la hora de inicio es 12:00:00 AM y la hora de término es 11:59:59 PM, con una diferencia de un segundo. Un horario que pasa la medianoche debe ser configurado de esta manera, porque si se introduce 12:00 AM como hora de inicio y fin, el programa se activa durante solo 59 segundos (12:00:00-12:00:59).

Intervalos de tiempo

Un intervalo es el período de tiempo durante el cual un horario está activo. goEntry puede asignar varios intervalos a cada horario.

Por ejemplo, si el personal de limpieza de la oficina lava y aspira los pisos los miércoles, pero los demás días de la semana solo limpia los baños y los cestos de basura, necesitan tener acceso durante más horas el miércoles que los otros días de la semana. En este caso, se crea un intervalo para el miércoles y otro para los demás días de la semana.

Agregar un horario

1. Seleccionar ***Administración de acceso > Horarios.***
2. Hacer clic en [Añadir].
3. Escribir un nombre descriptivo en el campo **Nombre del horario**.
4. Crear intervalos para el horario.
    a. Para crear intervalos adicionales, hacer clic en [Añadir] en el panel Lista de intervalos.
    b. Hacer clic en la caja de selección correspondiente a cada día que se desea añadir al intervalo.
    c. Escribir los valores de la hora de inicio y de fin.
5. Hacer clic en **Grupos de feriados**
6. Seleccionar los grupos de feriados incluidos en este horario.

   NOTA: Los feriados son excepciones de los horarios normales de acceso. Al incluir un grupo de feriados en un horario se evita que el grupo de feriados lo anule. Por ejemplo, si se ha creado un grupo de feriados para los feriados bancarios y la oficina de la empresa cierra esos días, no se selecciona ese grupo de feriados para el horario relativo al nivel de acceso del personal de oficina. Sin embargo, si el departamento de despacho trabaja los feriados, se selecciona el grupo de feriados bancarios para el horario relativo al nivel de acceso del personal de despacho, a fin de evitar que el grupo de feriados bancarios anule el horario del departamento de despacho.
7. Hacer clic en [Aceptar cambios].

Agregar un intervalo a un horario

1. Seleccionar ***Administración de acceso > Horarios.***
2. Seleccionar el horario a modificar.
3. Crear intervalos para el horario.
    a. Para crear intervalos adicionales, hacer clic en [Añadir] en el panel Lista de intervalos.
    b. Hacer clic en la caja de selección correspondiente a cada día que se desea añadir al intervalo.
    c. Escribir los valores de la hora de inicio y de fin.
4. Hacer clic en [Aceptar cambios].

Eliminar un intervalo de un horario

1. Seleccionar ***Administración de acceso > Horarios.***
2. Seleccionar el horario a modificar.
3. Seleccionar el intervalo a eliminar.
4. Hacer clic en [Remover] en el panel Lista de intervalos.
5. Hacer clic en [Aceptar cambios].

Copiar un horario

1. Seleccionar ***Administración de acceso > Horarios.***
2. Seleccionar el horario a copiar.
3. Hacer clic en [Copiar].
4. Escribir un nombre descriptivo en el campo **Nombre del horario**.
5. Agregar, eliminar o modificar los intervalos de tiempo según sea necesario.

6. Hacer clic en [Aceptar cambios].

Eliminar un horario

1. Seleccionar ***Administración de acceso > Horarios.***
2. Seleccionar el horario a eliminar.
3. Hacer clic en [Remover].

   Aparece caja de diálogo Remover item.
4. Hacer clic en [Remover].

Creación de grupos de lectoras

Los grupos de lectoras son útiles cuando se tiene una gran cantidad de lectoras y puertas en las instalaciones. Los grupos de lectoras permiten agrupar varias lectoras según una característica en común y asignarlas, como un grupo, a los niveles de acceso. Por ejemplo, todas las lectoras en el sótano de un edificio pueden agregarse a un grupo.

El agrupamiento no necesita estar relacionado con una zona física Por ejemplo, un grupo de lectoras llamado limpieza se puede usar en un nivel de acceso que autoriza el acceso a todos los armarios de almacenamiento de suministros de limpieza.

Los grupos de lectoras aparecen en la página Niveles de acceso, lo que permite autorizar el acceso a todas las lectoras de un grupo con una sola selección, en vez de una por una.

Agregar un grupo de lectoras

1. Seleccionar ***Administración de acceso > Grupos de lectoras***.
2. Hacer clic en [Añadir].
3. Escribir un nombre descriptivo en el campo **Nombre del grupo de lectoras**.
4. Seleccionar cada lectora del grupo.
5. Hacer clic en [Aceptar cambios].

Copiar un grupo de lectoras

1. Seleccionar ***Administración de acceso > Grupos de lectoras***.
2. Seleccionar el grupo de lectoras a copiar.
3. Hacer clic en [Copiar].
4. Escribir un nombre descriptivo en el campo **Nombre del grupo de lectoras**.
5. Agregar o modificar la asignación de lectoras según las necesidades.
6. Hacer clic en [Aceptar cambios].

Eliminar un grupo de lectoras

1. Seleccionar ***Administración de acceso > Grupos de lectoras***.
2. Seleccionar el grupo de lectoras a eliminar.

3. Hacer clic en [Remover].

   Aparece caja de diálogo Remover item.
4. Hacer clic en [Remover].

Configuración de los niveles de acceso

Los niveles de acceso determinan a qué puertas y cuándo una credencial tiene acceso. Por ejemplo, si las instalaciones cuentan con una oficina y un depósito, y no se permite que el personal de oficina entre al depósito, se crea un nivel de acceso para el personal de oficina, que incluye solo las puertas de la zona de las oficinas.

La página Niveles de acceso se usa para asignar horarios a las lectoras y los grupos de lectoras. Luego, los niveles de acceso se asignan a las credenciales, determinando los días y horas en que la persona con esa credencial puede entrar a través de las lectoras en ese nivel de acceso.

Agregar un nivel de acceso

1. Seleccionar ***Administración de acceso*** > ***Niveles de acceso***.
2. Hacer clic en [Añadir].
3. Escribir un nombre descriptivo en el campo **Nombre del nivel de acceso**.
4. Seleccionar las lectoras y los grupos de lectoras a incluir en este nivel de acceso.
5. Seleccionar un horario para cada lectora seleccionada.
6. Hacer clic en [Aceptar cambios].

Copiar un nivel de acceso

Si hay una gran cantidad de lectoras, la creación de un nuevo nivel de acceso puede tardar mucho tiempo. Copiar un nivel de acceso permite volver a usar una configuración similar y hacer solo unas cuantas modificaciones para adaptarla al nuevo nivel de acceso.

1. Seleccionar ***Administración de acceso*** > ***Niveles de acceso***.
2. Hacer clic en el nivel de acceso a copiar.
3. Hacer clic en [Copiar].
4. Escribir un nombre descriptivo en el campo **Nombre del nivel de acceso**.
5. Modificar según sea necesario las lectoras y los grupos de lectoras de este nivel de acceso.
6. Borrar la casilla próxima a cualquier lectora que no se desea incluir en este nivel de acceso.
7. Hacer clic en [Aceptar cambios].

Remover un nivel de acceso

1. Seleccionar ***Administración de acceso*** > ***Niveles de acceso***.
2. Hacer clic en el nivel de acceso a remover.
3. Hacer clic en [Remover].

   Aparece caja de diálogo Remover item.
4. Hacer clic en [Remover].

Configuración de roles de operador

Un rol de operador es una directiva de permisos de grupo. Cuando se agrega una persona y se le otorga la capacidad de iniciar sesión en goEntry y operarlo, se le conceden determinados permisos para modificar, ejecutar o simplemente ver recursos y datos. En lugar de configurar manualmente el acceso a cada recurso o dato para cada operador individual, el recurso de roles de operador permite asignar privilegios de acceso comunes a cada tipo de operador, según sus roles laborales específicos. goEntry incluye cinco roles predefinidos:

- **Solo ver**
- **Guarda**
- **Operador**
- **Distribuidor**
- **Administrador**

No se puede borrar ninguno de los cinco roles predefinidos, pero cuatro pueden modificarse. También se pueden crear funciones personalizadas. Se pueden borrar los roles personalizados, a menos que estén asignados a algún usuario.

Agregar un rol de operador

1. Seleccionar ***Administración del sistema > Roles de operador***.
2. Hacer clic en [Añadir].
3. Escribir un nombre descriptivo en el campo **Nombre de rol**.
4. Seleccionar un **permiso** para cada recurso.
5. Hacer clic en [Aceptar cambios].

Modificar un rol de operador

Nota: La función de administrador no puede modificarse.

1. Seleccionar ***Administración del sistema > Roles de operador***.
2. Para cambiar el nombre, escribir un nombre descriptivo en el campo **Nombre de rol**.
3. Cambiar el **permiso** para cada característica, según sea necesario.
4. Hacer clic en [Aceptar cambios].

Copiar un rol de operador

Copiar un rol de operador permite volver a usar una configuración similar y hacer solo unas cuantas modificaciones para adaptarla al nuevo rol de operador.

1. Seleccionar ***Administración del sistema > Roles de operador***.
2. Hacer clic en el rol de operador a copiar.
3. Hacer clic en [Copiar].
4. Escribir un nombre descriptivo en el campo **Nombre de rol**.
5. Cambiar el **permiso** para cada característica, según sea necesario.
6. Hacer clic en [Aceptar cambios].

Eliminar un rol de operador

Nota: No se puede eliminar ninguno de los cinco roles predefinidos.

1. Seleccionar ***Administración del sistema > Roles de operador***.
2. Hacer clic en el rol de operador por remover.
3. Hacer clic en [Remover].
   Aparece la caja de diálogo Remover Item.
4. Hacer clic en [Remover].

Configuración de Campos definidos por usuario

El registro de personas en la base de datos de goEntry puede tener campos definidos por el usuario. Esto permite introducir datos personales de los empleados, tales como el número de matrícula del vehículo o el número de teléfono particular. El campo debe estar habilitado para aparecer en la página Personas. Si se deshabilita un campo, se remueve de la base de datos y se pierden los datos correspondientes contenidos en el registro de cada persona.

Todas las bases de datos deben poder distinguir un registro de otro. Ya que algunos nombres son muy comunes, usar los apellidos de los empleados como identificador exclusivo de los registros de la base de datos no funciona. Por consiguiente, las organizaciones asignan a cada empleado un número de identificación exclusivo.

IMPORTANT: En goEntry, para obtener los mejores resultados, hay que definir un identificador de registros personales, como un número de empleado, exclusivo para cada persona en la organización. Sin una forma de identificar cada registro como exclusivo, las actualizaciones, importaciones, exportaciones y otras acciones de mantenimiento de la base de datos pueden dar lugar a que se modifique un registro incorrecto.

Al crear campos definidos por el usuario, se puede declararlos protegidos. La configuración de esta opción determina si los campos definidos por el usuario con la característica Protegido seleccionada son visibles o modificables por diferentes roles de operador. De este modo se aumenta el nivel de protección de la información confidencial, tal como números de teléfono particular. Por ejemplo, si se desea que los usuarios con el rol de operador vean toda la información personal y los usuarios con el rol de guarda vean solo la información personal no protegida, es necesario cambiar la configuración de los roles de operador como se muestra en la siguiente tabla:

Rol	Ajustes de campos definidos por usuario	Ajustes campos de usuario protegidos
Opera-dor	Solo ver	Solo ver
Guarda	Solo ver	Ninguno

Añadir campos definidos por usuario

Los campos definidos por usuario forman parte de los registros personales de la base de datos de goEntry. El campo debe estar habilitado para aparecer en la página Personas.

1. Seleccionar ***Administración del sistema > Ajustes del sistema***.
2. Hacer clic en la etiqueta **Campos definidos por usuario**.
3. Para cada campo:
   a. Seleccionar **Habilitado**.
   b. Escribir una **Etiqueta**.
   c. Opcional: seleccionar **Requerido**.
   d. Opcional: seleccionar **Protegido**.
4. Hacer clic en [Aceptar cambios].

Reorganizar campos definidos por usuario

Los campos definidos por usuario forman parte de los registros personales de la base de datos de goEntry. El campo debe estar habilitado para aparecer en la página Personas. Si se deshabilita un campo, se remueve de la base de datos y se pierden los datos correspondientes contenidos en el registro de cada persona.

IMPORTANTE: No se modifican las etiquetas de los campos para tratar de cambiar su orden. Los datos están asociados al campo, no a la etiqueta del campo. Cambiar la etiqueta no cambia el orden, pero da lugar a que los datos estén mal etiquetados.

1. Seleccionar ***Administración del sistema > Ajustes del sistema***.
2. Hacer clic en la etiqueta **Campos definidos por usuario**.
3. Usar las flechas Ordenar para mover los campos hacia arriba o hacia abajo.

   El orden de los campos en esta etiqueta coincide con el orden de los campos en la página Personas.

Eliminar un campo definido por el usuario

El campo debe estar habilitado para aparecer en la página Personas. Si se deshabilita un campo, se remueve de la base de datos y se pierden los datos correspondientes contenidos en el registro de cada persona.

1. Seleccionar ***Administración del sistema > Ajustes del sistema***.
2. Hacer clic en la etiqueta **Campos definidos por usuario**.
3. Borrar la caja **Habilitado** correspondiente al campo y los datos a borrar.
4. Hacer clic en [Aceptar cambios].

Comportamiento programación de puertas y lectoras

La etiqueta Ver horario, de la página Puertas, anula el comportamiento por default de puertas y lectoras de acuerdo con un horario. Por ejemplo, durante el horario comercial, debe haber una puerta desbloqueada para el acceso del público a la sala de exposición o el local de venta al por menor. Después del horario comercial normal, puede ser necesario que ciertas lectoras requieran una

credencial y un PIN (útil para impedir el acceso con tarjetas perdidas o robadas), de modo que se configura la lectora para solicitar, por default, solo una credencial (***Administración del sistema > Dispositivos***) y solicitar una credencial y un PIN después del horario comercial (***Monitoreo > Puertas > Ver horarios***).

Nota: No confundir el comportamiento de la puerta y la lectora con el acceso. La página Niveles de acceso se usa para asignar horarios a lectoras y a grupos de lectoras. Luego, los niveles de acceso se asignan a las credenciales, determinando los días y horas en que la persona con esa credencial puede entrar a través de las lectoras en ese nivel de acceso. El modo de acceso, solo credencial o credencial y PIN, no es relevante para el nivel de acceso. (Ver **Configuración de seguridad en pág. 14.**)

1. Seleccionar ***Monitoreo > Puertas***.
2. Hacer clic en la etiqueta **Ver horarios**.
3. Para cada combinación de puerta y lectora:
   a. Seleccionar un **Horario**.
   b. Seleccionar un **Modo de horario**.

      Para las puertas, los modos de horario son:
      - **Desbloqueada**
      - **Primera entrada con tarjeta**
      - **Bloqueada**

      Para las lectoras, los modos de horario son:
      - **Solo credencial**
      - **Credencial y PIN**

Importar personas y credenciales de un archivo CSV

El Asistente de importación/exportación permite asignar los campos de un archivo de valores separados por coma (CSV) a la tabla de la base de datos de goEntry, e importar personas y credenciales.

Nota: Un registro personal goEntry se compone de campos definidos por el usuario para la información personal, las credenciales de acceso (tarjeta de ID, PIN, nivel de acceso) e información opcional sobre la cuenta de usuario que permite iniciar sesión en goEntry. Es imposible importar/exportar de goEntry datos de cuenta de usuario. Solo se pueden importar/exportar datos personales y de credenciales definidos por el usuario.

Ver "Importar personas y credenciales de un archivo CSV" en el *Manual del usuario del Asistente de importación/exportación goEntry*.

Crear un respaldo y un punto de restauración

Una vez completada la configuración de goEntry, es importante crear un archivo de respaldo, almacenado en la PC local, y un punto de restauración (salvar configuraciones personalizadas) almacenado en el controlador, en caso de tener que restaurar el sistema a su estado inicial de operación.

Ver **Prevención de pérdida de datos en pág. 57.**

CAPÍTULO 4 *Administración de Acceso*

Administra acceso a las instalaciones y a goEntry, para:

- Añadir y remover personas
- Añadir, desactivar, reactivar y remover credenciales
- Añadir y eliminar cuentas de usuario

Administración de Personas

Cada persona en la organización puede tener acceso al edificio y a goEntry. El acceso a las instalaciones físicas se controla con una credencial (tarjeta de identificación). El acceso a goEntry se controla por medio de una cuenta de usuario para iniciar sesión en el controlador. Para mantener organizadas las credenciales y cuentas de usuario, goEntry las asocia con el registro de cada persona que forma parte de la organización. Este registro individual en la base de datos se llama "persona", porque corresponde a una persona real.

Es importante distinguir entre las personas, las credenciales y las cuentas de usuario. En primer lugar, todos los que necesitan entrar en las instalaciones necesitan una credencial (una tarjeta de identificación con un número codificado que goEntry reconoce). Sin embargo, no todos los que necesitan tener acceso a las instalaciones necesitan también tener acceso a goEntry con una cuenta de usuario. En segundo lugar, solo los que operan y administran goEntry necesitan cuentas de usuario. En tercer lugar, en algunos casos, los operadores de goEntry se encuentran fuera de las instalaciones en una estación central y, por lo tanto, no necesitan una credencial para acceder a las instalaciones físicas, a pesar de que tienen una cuenta de usuario.

Los registros de la base de datos, "personas", de goEntry permiten administrar convenientemente las credenciales y cuentas de usuario en un registro, en lugar de mantener bases de datos separadas para los usuarios del sistema y las credenciales de acceso a instalaciones.

Agregar una persona

Asignar a cada registro personal un número de identificación individual de algún tipo. Puede ser el número de empleado, por ejemplo.

Antes de agregar personas, configurar todos los campos definidos por el usuario que sean necesarios. Ver **Añadir campos definidos por usuario en pág. 37.**

1. Hacer clic en ***Administración de acceso > Personas***.
2. Hacer clic en [Añadir].
3. Escribir un **nombre** y un **apellido**.
4. Hacer clic en la etiqueta **Detalles**.
5. Escribir la información solicitada en los campos definidos por el usuario.
6. Si la persona va a usar el software goEntry, hacer clic en la etiqueta **cuentas de usuario** y crear la cuenta. Ver **Añadir una cuenta de usuario en pág. 43.**
7. Hacer clic en [Aceptar cambios].
8. Si la persona requiere una credencial de acceso a las instalaciones físicas, consultar Añadir una credencial en pág. 41.

Remover una persona

goEntry puede almacenar hasta 10,000 registros de personas. Sin embargo, las personas que ya no requieren acceso a las instalaciones o a goEntry deben eliminarse de la base de datos.

Nota: Para eliminar varias personas en un solo lote, usar el Asistente de importación/exportación.

1. Hacer clic en ***Administración de acceso > Personas***.
2. En la lista de personas, seleccionar la persona.
3. Hacer clic en [Remover].

   Aparece caja de diálogo Remover item.
4. Hacer clic en [Remover].

Cargar fotos de identificación de la persona

Las personas pueden tener una foto de identificación asociada a su registro. Una miniatura de esta foto aparecerá cada vez que se produce un evento de acceso relativo a la credencial de la persona.

El tamaño de las fotos no puede ser de más de 10 KB.

1. Hacer clic en ***Administración de acceso > Personas***.
2. En la lista de personas, seleccionar la persona.
3. Hacer clic en el ícono de la foto de identificación que se encuentra al lado del nombre de la persona.

   Aparece el cuadro de diálogo Cargar foto.
4. Hacer clic en **Seleccionar archivo**.

   Aparece la caja de diálogo Seleccionar archivo.
5. Seleccionar la foto a cargar y hacer clic en **Abrir.**
6. Hacer clic en **Cargar**.

7. Desaparece la caja de diálogo Seleccionar archivo.
8. Hacer clic en [Aceptar cambios].

Nota: Se puede reemplazar una foto de identificación de usuario con una foto actualizada, haciendo clic en la foto actual y siguiendo los pasos anteriores.

Administración de credenciales

Todos los que necesitan entrar en las instalaciones necesitan una credencial (una tarjeta de identificación con un número codificado que goEntry reconoce). Antes de poder asignar una credencial, es necesario agregar a la persona a la base de datos. Ver **Agregar una persona en pág. 40.**

Añadir una credencial

Antes de agregar una credencial a una persona, es necesario crear un registro de esa persona. Ver **Agregar una persona en pág. 40.**

1. Hacer clic en ***Administración de acceso > Personas***.
2. Seleccionar la persona que necesita la credencial.
3. Hacer clic en [Credenciales].
4. Hacer clic en [Añadir credencial].
5. Hacer clic en la etiqueta **General**.
6. Escribir la **identificación de la credencial**.
7. Opcional: escribir el código **PIN**.
8. Opcional: seleccionar **Usar tiempo extendido mantenido/abierto** si la persona titular de la credencial necesita más tiempo para abrir y pasar por las puertas.
9. Opcional: seleccionar **Exento de Anti-passback**, si se usa la función Anti-passback y esta credencial no ha de rastrearse.
10. Opcional: seleccionar una fecha de **activo desde** y **activo hasta**, si la credencial tiene validez temporal.
11. Hacer clic en la etiqueta **Niveles de acceso**.
12. Seleccionar los niveles de acceso correspondientes a la credencial.
13. Hacer clic en [Aceptar cambios].

Lectoras de credenciales USB

RF Ideas fabrica lectoras de credenciales que pueden conectarse a una computadora por USB. Estos dispositivos se pueden usar para leer los datos almacenados en una tarjeta de identificación e insertar automáticamente la credencial en el campo **ID de credencial**. De modo que ahorra un tiempo considerable si es necesario agregar muchas credenciales a goEntry.

Estos dispositivos deben instalarse y configurarse de acuerdo con las instrucciones del fabricante y si se usan credenciales con código de instalación, las lectoras de RF deben configurarse de modo de separar el código de instalación del código de la credencial en la tarjeta.

Remover una credencial

No es necesario remover una credencial para evitar su uso. Por ejemplo, si una persona reporta la pérdida de una credencial, en lugar de eliminar la credencial de inmediato, se puede desactivarla hasta que la persona haya tenido tiempo de buscarla. Si no la encuentra, entonces, cuando la persona solicita una nueva credencial, se remueve la credencial perdida. Ver **Evitar el uso de una credencial perdida o robada en pág. 42.**

1. Hacer clic en ***Administración de acceso > Personas***.
2. Seleccionar la Persona titular de la credencial por borrar.
3. Hacer clic en [Credenciales].
4. Hacer clic en la credencial por borrar.
5. Hacer clic en [Remover credencial].
6. Hacer clic en [Remover].

   Aparece caja de diálogo Remover item.
7. Hacer clic en [Remover].

Administración de credenciales perdidas o robadas

Si una persona reporta la pérdida de una credencial, en lugar de eliminar la credencial de inmediato, se puede desactivarla hasta que la persona haya tenido tiempo de buscarla. Si no la encuentra, entonces, cuando la persona solicita una nueva credencial, se remueve la credencial perdida.

La desactivación de una credencial tiene otra ventaja. Dado que cualquier credencial no válida que pase por una lectora genera un evento, si la credencial todavía está asignada a una persona, el evento indica específicamente tal persona como tratando de usar una credencial no válida. Si hay cámaras de video monitoreando los eventos de las puertas y las lectoras, se tiene una imagen de la persona que intentó usar la credencial después que fue reportada como robada. Una búsqueda en la base de datos de eventos de la persona que perdió la credencial muestra todos los incidentes relacionados con esa persona antes y después de que la credencial fuera reportada como perdida. De esta manera, se puede ayudar a establecer una asociación entre la víctima y el autor del robo.

Evitar el uso de una credencial perdida o robada

Usar esta tarea para desactivar una credencial en vez de eliminarla.

1. Seleccionar ***Administración de acceso > Personas***.
2. Seleccionar la persona titular de la credencial a desactivar.
3. Hacer clic en [Credenciales].
4. Hacer clic en la credencial a desactivar.
5. Hacer clic en el campo **Activo hasta**.

   Aparece la ventana emergente del calendario.
6. Seleccionar una fecha pasada.
7. Hacer clic en [Aceptar cambios].

Restaurar una credencial encontrada

1. Seleccionar ***Administración de acceso > Personas***.
2. Seleccionar la persona titular de la credencial a desactivar.
3. Hacer clic en [Credenciales].
4. Hacer clic en la credencial a reactivar.
5. **Borrar** el campo **Activo hasta**.
6. Hacer clic en [Aceptar cambios].

Administración de cuentas de usuario

Las cuentas de usuario permiten iniciar sesión en goEntry. Una cuenta de usuario está asociada con el registro de una persona en la base de datos, al igual que una credencial. Sin embargo, las personas no necesitan tener una cuenta de usuario para tener acceso a las instalaciones con una credencial.

Añadir una cuenta de usuario

1. Iniciar sesión como administrador o distribuidor. Los roles de los otros operadores no tienen permiso para modificar cuentas de usuario.
2. Seleccionar ***Administración de acceso > Personas***.
3. Seleccionar a la persona a modificar.
4. Hacer clic en la etiqueta **Cuenta de usuario**.
5. Seleccionar **Puede iniciar sesión**.
6. Escribir un **Nombre de usuario**.
7. Hacer clic en [Cambiar contraseña].
8. Escribir la nueva contraseña en los campos **Ingresar nueva contraseña** y **Confirmar contraseña**.
9. Hacer clic en [OK].
10. Seleccionar un **Rol**.
11. Hacer clic en [Aceptar cambios].

Cambiar un nombre de usuario y contraseña

1. Iniciar sesión como administrador o distribuidor. Los roles de los otros operadores no tienen permiso para modificar cuentas de usuario.
2. Seleccionar ***Administración de acceso > Personas***.
3. Seleccionar a la persona a modificar.
4. Hacer clic en la etiqueta **Cuenta de usuario**.
5. Escribir un nuevo **Nombre de usuario**.
6. Hacer clic en [Cambiar contraseña].
7. Escribir la nueva contraseña en los campos **Ingresar nueva contraseña** y **Confirmar contraseña**.
8. Hacer clic en [OK].
9. Hacer clic en [Aceptar cambios].

Desactivar una cuenta de usuario

1. Iniciar sesión como administrador o distribuidor. Los roles de los otros operadores no tienen permiso para modificar cuentas de usuario.
2. Seleccionar ***Administración de acceso > Personas***.
3. Seleccionar a la persona a modificar.
4. Hacer clic en la etiqueta **Cuenta de usuario**.
5. Limpiar la caja de selección **Puede iniciar sesión**.
6. Hacer clic en [Aceptar cambios].

Reportes

goEntry tiene cinco reportes predefinidos que permiten ver la información almacenada en la base de datos del servidor:

Historial de acceso
Permite ver un resumen de los intentos de acceso por persona, filtrado por intervalo de fechas, nombre de persona (comodín), lectora, área y autorizado o denegado.

Credencial
Permite ver una lista de credenciales asignadas, filtrada por nombre de persona (comodín), identificación de la credencial (comodín), nivel de acceso, activa o inactiva.

Acceso a lectoras
Permite ver una lista de personas con acceso a cada lectora, filtrada por nombre de persona (comodín) y lectora.

Lista de asistencia
Permite ver una lista de personas por área actual o última lectora, filtrada por nombre de persona (comodín), área y lectora.

Nómina
Permite ver una lista de todas las personas en la base de datos, filtrada por nombre de persona (comodín) y privilegios de inicio de sesión.

Nota: Los reportes se muestran en formato HTML, en una ventana del navegador de Internet. El logotipo del producto goEntry aparece en la esquina superior derecha. Si se usa Internet Explorer 7 o una versión anterior, esta imagen no se visualizará correctamente. Esta es una limitación de las versiones anteriores de Internet Explorer.

Búsqueda de personas

La función de búsqueda filtra la base de datos haciendo una lista de los registros de personas con un campo que coincide en todo o en parte con los requisitos de la búsqueda.

Buscar personas

1. Seleccionar ***Administración de acceso > Personas***.
2. Hacer clic en el botón **Buscar** para seleccionar el campo de búsqueda.
3. Escribir el término a buscar.
4. Presionar <Ingresar>.

Cancelar la búsqueda

Los resultados de la búsqueda continúan a filtrar la base de datos, incluso si se pasa a otra página y se vuelve a la página Personas, hasta que se cancela la búsqueda.

1. Seleccionar ***Administración de acceso > Personas***.
2. Hacer clic en la **X** para borrar el campo de búsqueda.

CAPÍTULO 5

Monitoreo del Acceso

Durante las operaciones del día a día, se monitorea y controla el acceso a las instalaciones por medio de:

- Visualización de eventos
- La visualización de videos de las cámaras de seguridad, si se han instalado cámaras
- La anulación del comportamiento programado de las puertas, en la medida que sea necesario abrirlas, desbloquearlas, bloquearlas o restablecerlas
- La respuesta a las alarmas

Eventos y alarmas

La página Eventos recoge el registro de:

- Problemas de acceso
    - Acceso no autorizado
    - Violaciones de Anti-passback
    - Puertas mantenidas abiertas demasiado tiempo
    - Usuarios con sesión iniciada en goEntry
- Mensajes de estado del sistema y los dispositivos
    - Cambios en el estado del sistema, tales como actualizaciones de la hora y fecha
    - Cambios de modo de los dispositivos conectados
- Alarmas
    - Sabotaje de puertas
    - Puertas apertura forzada
    - Fallas o problemas del sistema

Todo evento asociado a un dispositivo conectado a una cámara tiene un registro en video del evento.

Ver últimos eventos

Los últimos eventos se muestran en la esquina inferior izquierda de la página. Si se produce un evento mientras se está trabajando en otra página, pasando el cursor sobre el evento, se puede ver un resumen del evento, que incluye una foto en miniatura de la persona implicada.

La ventana emergente muestra la fecha y hora del evento, una descripción del evento y la credencial. Debajo de eso aparece la foto y el nombre de la persona.

Cargar más eventos

La pantalla Eventos solo muestra los últimos eventos. Para ver eventos más antiguos que los que se muestran, hay que cargarlos al navegador desde goEntry. El comando Cargar más eventos cargará los próximos 500 eventos (o menos, si hay menos de 500).

1. Seleccionar ***Eventos***.
2. Hacer clic en el botón de mando **Eventos**.
3. Seleccionar **Cargar más eventos**.
4. Opcional: para detener la operación, hacer clic en **Cancelar**, cuando aparezca.

Cargar todos los eventos

La pantalla Eventos solo muestra los últimos eventos. Para ver eventos más antiguos que los que se muestran, hay que cargarlos al navegador desde goEntry. El comando Cargar todos los eventos carga todos los eventos del controlador al navegador y puede tardar varios minutos en completarse.

1. Seleccionar ***Eventos***.
2. Hacer clic en el botón de mando **Eventos**.
3. Seleccionar **Cargar más eventos**.
4. Opcional: para detener la operación, hacer clic en **Cancelar**, cuando aparezca.

Búsqueda de Eventos

La función de búsqueda permite filtrar la lista de eventos exhibidos por una o más facetas.

1. Seleccionar ***Eventos***.
2. Hacer clic en el ícono **Filtro**, que se encuentra en el lado derecho de la pantalla.
3. Escribir los criterios de búsqueda en los campos correspondientes.

   Cuanto más criterios se usan, más preciso es el resultado de la búsqueda.
4. Presionar <Ingresar>.

Exportar eventos

goEntry puede almacenar hasta 65,535 eventos. Una vez que se alcanza este límite, se eliminan los eventos más antiguos, según sea necesario para hacer espacio. Usar el comando Exportar eventos para almacenar un registro de eventos en formato de valores separados por comas (CSV).

1. Seleccionar ***Eventos***.
2. Hacer clic en el botón de mando **Eventos**.
3. Seleccionar **Exportar eventos**.
4. Elegir la ubicación en la computadora en donde se guardará el archivo.

5. Escribir un nombre descriptivo con la extensión **.csv**.
6. Hacer clic en **Guardar**.

Video de eventos

goEntry puede mostrar video en directo (o grabado) de cámaras específicas y asociar videos grabados a eventos registrados de dispositivos específicos, tales como lectoras y puertas. Ver **Configuración de dispositivos de video en pág. 25.**

Los enlaces a videos de eventos específicos se encuentran en la página Eventos. La página Video permite monitorear en directo el video de una o más cámaras.

Reproducir video de eventos

En la página Eventos, los eventos con video grabado asociado tienen un icono hipervinculado de una cámara al lado de la descripción del evento.

FIGURA 1. **Icono cámara de video del evento**

1. Seleccionar ***Eventos***.
2. Desplazarse o buscar el evento.
3. Hacer clic en el ícono de la cámara.

   El panel Detalle de eventos aparece en la parte inferior de la página.
4. Hacer clic en [Reproducir video del evento].

Monitorear video

Mientras que la pantalla Eventos permite ver videos grabados de eventos vinculados a dispositivos específicos, la página Video permite monitorear la seguridad general de las instalaciones. Por ejemplo, si una persona sospechosa estuviera acechando el estacionamiento, no daría lugar a un evento de puerta o lectora, pero si hay una cámara de vigilancia en el estacionamiento, se podría detectar la presencia de tal persona mirando el video de dicha cámara.

Antes de monitorear videos en directo o grabados, se debe agregar al menos una plantilla de video. Ver **Agregar plantillas de video en pág. 27.**

1. Seleccionar ***Monitoreo > Video***.
2. Seleccionar una **plantilla**.
3. Para ver video en directo, pulsar el botón **Directo**.
4. Para ver videos grabados, hacer clic en la lista **Reproducción** y seleccionar una opción.
5. Opcional: Para reposicionar una cámara con movimiento horizontal, vertical y zoom, hacer clic en el botón **PTZ** para abrir y ajustar los controles de movimiento horizontal, vertical y zoom.

Referencia controles de video

Icono	Característica	Función
	Control del iris	abre o cierra el iris de la cámara para ajustarlo a la cantidad de luz disponible
	Control del foco	ajusta el foco de la imagen
	Control de zoom	ajusta el zoom de la cámara
	Controles de movimiento horizontal y vertical	Mueve la cámara en la dirección indicada por la flecha correspondiente
	Control de retroceso cuadro a cuadro	Retrocede un cuadro el video grabado
	Control de retroceso	Retrocede el video
	Control de pausa	Detiene la transmisión de video (en vivo o grabado)
	Control de avance	Avanza el video grabado en avance rápido
	Control de avance cuadro a cuadro	Avanza un cuadro el video grabado
	Control de video en vivo	Cambia de reproducción de video grabado a visualización de video en vivo
	Control de reproducción	Menú de selección de opciones de reproducción, desde en vivo a varios minutos anteriores

Icono	Característica	Función
	Control de preajustes	Mueve la cámara rápidamente a la posición preajustada
	Control PTZ	Abre los controles de movimiento horizontal,vertical y zoom (solo funciona con cámaras PTZ)

Control de puertas

La página **Puertas** muestra el estado de las puertas, las lectoras asignadas, los eventos recientes en esas puertas y los horarios asignados. La página **Puertas** permite que los operadores bloqueen, abran, restablezcan y desbloqueen las puertas.

Abrir una puerta

Usar el comando Abrir puerta para abrir una puerta para alguien sin credencial.

1. Seleccionar ***Monitoreo > Puertas***.
2. Hacer clic en la etiqueta **Ver eventos**.
3. Pulsar el botón de mando **Comandos de puerta individual** correspondiente a la puerta que se desea abrir.
4. Seleccionar **Abrir puerta**.

Restablecer una puerta

Usar el comando Restablecer puerta para volver la puerta a su modo normal de funcionamiento, tras bloquearla o desbloquearla.

1. Seleccionar ***Monitoreo > Puertas***.
2. Hacer clic en la etiqueta **Ver eventos**.
3. Pulsar el botón de mando **Comandos de puerta individual** correspondiente a la puerta que se desea restablecer.
4. Seleccionar **Restablecer puerta**.

Bloquear una puerta

Usar el comando Bloquear puerta para impedir el acceso de cualquier credencial por esa puerta.

1. Seleccionar ***Monitoreo > Puertas***.
2. Hacer clic en la etiqueta **Ver eventos**.
3. Pulsar el botón de mando **Comandos de puerta individual** correspondiente a la puerta que se desea bloquear.
4. Seleccionar **Bloquear puerta**.

Desbloquear una puerta

Usar el comando Desbloquear puerta para anular la seguridad de la puerta, permitiendo que cualquiera pueda salir o entrar sin presentar una credencial válida.

1. Seleccionar ***Monitoreo > Puertas***.
2. Hacer clic en la etiqueta **Ver eventos**.
3. Pulsar el botón de mando **Comandos de puerta individual** correspondiente a la puerta que se desea desbloquear.
4. Seleccionar **Desbloquear puerta**.

Restablecer todas las puertas

Usar el comando Restablecer todas las puertas para volver todas las puertas a su modo normal de funcionamiento, tras bloquear o desbloquear todas las puertas.

1. Seleccionar ***Monitoreo > Puertas***.
2. Pulsar el botón de mando **Comandos globales de puertas**, que se encuentra en la parte superior de la página.
3. Seleccionar **Restablecer todas las puertas**.

Bloquear todas las puertas

Usar el comando Bloquear todas las puertas para impedir el acceso de todas las credenciales en todas las puertas.

1. Seleccionar ***Monitoreo > Puertas***.
2. Pulsar el botón de mando **Comandos globales de puertas**, que se encuentra en la parte superior de la página.
3. Seleccionar **Bloquear todas las puertas**.

Nota: Aunque todas las puertas estén bloqueadas al agregar un nuevo controlador de puerta, éste permanecerá desbloqueado. Para bloquearlo, se deben restablecer todas las puertas para bloquearlas a todas nuevamente.

Desbloquear todas las puertas

Usar el comando Desbloquear todas las puertas para anular la seguridad de todas las instalaciones, permitiendo que cualquiera pueda salir o entrar sin presentar una credencial válida.

1. Seleccionar ***Monitoreo > Puertas***.
2. Pulsar el botón de mando **Comandos globales de puertas**, que se encuentra en la parte superior de la página.
3. Seleccionar **Desbloquear todas las puertas**.

Menú Comandos de puertas

A veces es necesario anular el comportamiento normal programado de una puerta específica o de todas las puertas. Por ejemplo, puede ser necesario abrir una puerta a una persona que entrega un paquete. Durante un simulacro de incendio, es necesario desbloquear todas las puertas para facilitar el ejercicio. Si se produce un desastre o una emergencia cerca de las instalaciones, tal vez sea necesario bloquear todas las puertas. Se pueden controlar puertas individuales desde la etiqueta **Ver eventos** de

la página ***Monitoreo > Puertas***. Los comandos globales de puertas permiten cambiar con un solo clic el estado de todas las puertas de las instalaciones.

Menú Comandos globales de puertas

Nota: Después de bloquear o desbloquear todas las puertas, se debe usar el comando **Restablecer todas las puertas**, antes de tratar de controlar cualquier puerta de forma individual.

Desbloquear todas las puertas
Libera las cerraduras de todas las puertas, permitiendo entrar y salir libremente. Esto se registra como Evento 14644. Después de emitir este comando, se debe restablecer todas las puertas antes de poder controlar directamente una puerta individual.

Bloquear todas las puertas
Bloquea todas las puertas e ignora las credenciales, de modo que nadie puede entrar ni salir. Esto se registra como Evento 14646. Después de emitir este comando, se debe restablecer todas las puertas antes de poder controlar directamente una puerta individual.

Restablecer todas las puertas
Restaura todas las puertas a su estado normal, a menos que esté activa una **entrada** de desbloqueo asignada. Se configura una entrada de desbloqueo en la página ***Administración del sistema > Dispositivos > Controlador***.

Menú Comandos de puerta individual

Abrir puerta.
Desbloquea la puerta durante el período especificado en **Hora de acceso normal autorizado**, en la página ***Administración del sistema > Dispositivos***.

Restablecer puerta.
Restaura la puerta al comportamiento predeterminado según el horario establecido.

Bloquear puerta
Bloquea las puertas e ignora las credenciales, de modo que nadie puede entrar ni salir.

Desbloquear puerta.
Libera la cerradura de la puerta, permitiendo entrar y salir libremente, hasta que se cambia el estado de la puerta, el horario de la lectora cambia el estado de puerta o se ejecuta un comando global (para todas las puertas).

Etiqueta Ver eventos

La etiqueta **Ver eventos** de la página ***Monitoreo > Puertas*** muestra el último evento de la puerta y las lectoras asociadas, y el estado actual de cada puerta y sus lectoras. Se pueden controlar puertas individuales desde la etiqueta **Ver eventos** de la página ***Monitoreo > Puertas***.

Etiqueta Ver horarios

La etiqueta **Ver horarios** de la página ***Monitoreo > Puertas*** permite modificar el comportamiento de las lectoras y las puertas de acuerdo con los horarios establecidos, en vez de manualmente como en la etiqueta **Ver eventos**.

Por ejemplo, si hay una sala de exposición de productos para los clientes, es conveniente que la puerta del estacionamiento a la sala de exposición permanezca bloqueada fuera del horario comercial, pero

desbloqueada durante el horario de atención al público, de modo que los clientes puedan entrar sin dificultad en el edificio. En este caso, es posible seleccionar un horario de 9.00 a 17.00 para la puerta y elegir la opción "Primera entrada con tarjeta" para el **Modo de horario**, si desea que la sala de exposiciones esté desbloqueada solo después de que un vendedor usa una credencial para entrar en ella.

Horario
En esta lista, seleccionar un horario (los horarios se crean en ***Administración de acceso > Horarios***) para indicar cuándo el Modo de horario seleccionado debe estar activo.

Modo de Horario (puerta)

Seleccionar una opción de esta lista para configurar el comportamiento de la puerta específica durante el horario especificado.

Desbloqueado
La puerta permanecerá desbloqueada y accesible sin la presentación de una credencial durante el horario seleccionado.

Primera entrada con tarjeta
La puerta estará bloqueada al principio del horario y permanecerá en este estado hasta que se pase una credencial válida. En ese momento, la puerta cambiará al estado desbloqueado.

Bloqueada
Durante el horario seleccionado, la puerta permanece cerrada y es necesario pasar una credencial válida para entrar.

Modo de horario (lectora)

Seleccionar una opción de esta lista para configurar el comportamiento de la lectora específica durante el horario especificado.

Solo Credencial
Para accesar, solo es necesario presentar una credencial válida (ID de Credencial).

Credencial y PIN
Para accesar, es necesario presentar una credencial válida y un número de identificación personal. Esto impide el acceso con una credencial robada o encontrada. Algunas instalaciones usan el modo **Solo credencial** durante el día y **Credencial y PIN** fuera del horario laboral, cuando las instalaciones están vacías.

Modo Puerta degradada

La información de las credenciales se almacenan en el controlador del sistema goEntry. Si un controlador de puertas no puede comunicarse con el controlador para determinar si debe autorizar el acceso (por ejemplo, por una mala conexión), las puertas conectadas a ese controlador de puertas funcionarán en modo degradado:

Restringido
No se autoriza ningún acceso.

Código de instalación
Se autoriza el acceso si la credencial coincide con uno de los formatos definidos en la página ***Administración del sistema > Formatos de tarjeta*** y el código de instalación en la tarjeta coincide con el definido para el formato. No se verifica la identidad de la credencial.

Todos
Se autoriza el acceso si la tarjeta coincide con cualquiera de los formatos definidos en la página ***Administración del sistema > Formatos de tarjeta***, independientemente del código de instalación y la identidad de la credencial.

Monitoreo de entradas y salidas

Las entradas y salidas son opciones generales que permiten personalizar goEntry a las necesidades de la organización. Una entrada puede ser la señal de un detector de movimiento, por ejemplo. Una salida es un impulso eléctrico enviado por el controlador goEntry a algún dispositivo. Las entradas y salidas se monitorean desde la página ***Monitoreo > Entradas/salidas***, desde donde se pueden activar manualmente las salidas.

Activar o desactivar una salida

1. Seleccionar ***Monitoreo > Entradas / salidas***.
2. Pulsar el botón Activar/desactivar correspondiente a la salida.

   El estado cambia de "desactivado" a "activado" o de "activado" a "desactivado".

Restablecer Anti-passback

La opción Anti-passback requiere el uso de una credencial para entrar y salir de una área. De esta forma, el sistema rastrea en qué área se encuentra el portador de la credencial, mantiene un registro de los movimientos del personal en áreas protegidas e impide el paso a las áreas lógicamente imposibles. Si una persona usa una credencial para entrar en una área configurada como Anti-passback y, luego, sale sin usar la credencial (a través de una puerta mantenida abierta por otra persona, por ejemplo), goEntry no registra la salida del área específica de esa persona. Como resultado, si goEntry está configurado para imponer con rigor el Anti-passback, impide que esa credencial se use para entrar en otra área, incluida la que acabó de dejar, hasta que la ubicación de la credencial se restablece a un área neutra o predeterminada.

1. Seleccionar ***Monitoreo > Restablecimiento Anti-passback***.
2. Para restablecer todas las personas:
   a. Hacer clic en [Restablecer todo].
   b. Seleccionar un área de la lista.
3. Para restablecer a personas seleccionadas:
   a. Seleccionar un intervalo de personas haciendo clic en el primer nombre de la lista y, luego, mantener apretada la tecla <Mayús>, mientras se hace clic en la última persona. El intervalo de nombres se resalta.
   b. Seleccionar personas individuales haciendo clic en el primer nombre deseado y, luego, mantener apretada la tecla <Ctrl>, mientras se hace clic en los otros nombres para seleccionarlos.
   c. Hacer clic en [Restablecer lo seleccionado].
   d. Seleccionar un área de la lista.

CAPÍTULO 6 *Mantenimiento*

Unas pocas actividades simples de mantenimiento ayudan a garantizar que el sistema goEntry funcione en forma eficiente con el mínimo de problemas e interrupciones. Entre ellas se encuentran respaldar la base de datos y la configuración del controlador, actualizar el firmware (software de interfaz de usuario goEntry instalado en el controlador del sistema goEntry).

Iniciar sesión en goEntry

1. Abrir el navegador de Internet
2. Iniciar sesión en goEntry.
   a. Escribir direcciones IP para goEntry en la barra direcciones del navegador.
   b. Si al usar Internet Explorer recibe una advertencia sobre el certificado de seguridad, seleccionar **Pasar a este sitio web (no recomendado)**.
   c. Escribir **Nombre usuario**.
   d. Escribir **Contraseña**.
   e. Seleccionar **Idioma**.
   f. Hacer clic en [Iniciar sesión].

Prevención de pérdida de datos

Se recomienda respaldar periódicamente la base de datos de goEntry, para asegurar la recuperación rápida de sus necesidades de seguridad tras un desastre. Guardar archivo de respaldo en la computadora local, para conservar una copia fuera del controlador goEntry. El archivo de respaldo es encriptado. El archivo de respaldo incluye todos los registros y los parámetros configurables en goEntry, salvo:

- Ajustes de configuración de la red
- Estados de puerta/lectora ajustados manualmente a través de la página Puerta

Crear una copia de respaldo

1. Iniciar sesión en goEntry.
2. Seleccionar ***Administración del sistema > respaldo/restauración de la base de datos***.
3. Hacer clic en [Descargar archivo de respaldo].
   Aparece la caja de diálogo respaldo base de datos.
4. Hacer clic en [Descargar archivo de respaldo].
5. Seleccionar una ubicación para el archivo.
6. Hacer clic en [Salvar].

Restaurar a partir de un respaldo

IMPORTANTE: La restauración del respaldo sobrescribe la base de datos y se pierden todos los cambios realizados desde la fecha del respaldo.

1. Iniciar sesión en goEntry.
2. Seleccionar ***Administración del sistema > respaldo/restauración de la base de datos***.
3. Hacer clic en [Buscar].
4. Ir al archivo de respaldo.
5. Seleccionar el archivo y hacer clic en [Abrir].
6. Hacer clic en [Cargar archivo de respaldo].

Salvar y restablecer la configuración personalizada

A diferencia de un archivo de respaldo, la configuración personalizada se almacena en el controlador del sistema goEntry. El archivo de ajustes personalizados incluye todas las configuraciones y los datos. Es como un estado personalizado por default. En lugar de regresar el controlador a los ajustes de fábrica, que luego tendría que reconfigurarse a las necesidades específicas del sistema, se puede salvar la configuración básica de las instalaciones como una configuración personalizada y reiniciar a esa configuración de ser necesario.

Salvar los ajustes personalizados

Esta tarea crea un archivo con todos los datos y ajustes de configuración de goEntry presentes, almacenados en el controlador del sistema goEntry.

1. Seleccionar ***Administración del sistema >Salvar/restablecer ajustes.***
2. Seleccionar **Salvar Ajustes personalizados**.
3. Escribir **Nombre usuario**.
4. Escribir **Contraseña.**
5. Escribir la frase de seguridad, tal y como se muestra (mayúsculas y minúsculas).
6. Hacer clic en **Salvar ajustes personalizados**.

Restablecer ajustes personalizados

IMPORTANTE: Al usar esta función, se borran todos los datos y ajustes configurados en goEntry y se restablece la configuración almacenada en el archivo de ajustes

personalizados. Antes de restablecer los ajustes personalizados, comprobar que hay una copia de respaldo actualizada.

IMPORTANTE: Tras la restauración de los ajustes personalizados, el controlador se reiniciará. Durante este tiempo estará fuera de línea durante unos minutos. Por lo tanto, es mejor usar esta función durante los períodos de poca actividad de acceso, o los tarjeta habientes se verán obligados a esperar para poder entrar, si no se ha configurado un **modo degradado de puerta** que permita el acceso cuando el controlador no está en línea.

1. Seleccionar ***Administración del sistema >Salvar/restablecer ajustes.***
2. Seleccionar **Restablecer ajustes personalizados**.
3. Escribir **Nombre usuario**.
4. Escribir **Contraseña.**
5. Escribir la frase de seguridad, tal y como se muestra (mayúsculas y minúsculas).
6. Hacer clic en **Restablecer ajustes personalizados**.

   Aparece el siguiente mensaje de advertencia: “"Se está reiniciando el dispositivo" y se muestra una barra de progreso.

   Cuando la barra de progreso llega a su fin, el servidor sale de línea y el navegador muestra la página por default para cuando no puede conectarse a una dirección web.
7. Borrar la caché del navegador. (En Internet Explorer 8 o posterior, pulsar <Ctrl>+<Mayús>+<Supr>.)

Restablecer ajustes de fábrica

IMPORTANTE: Al usar esta característica, se borran todos los datos y parámetros configurados en goEntry y se restablecen los ajustes de fábrica. Antes de la restauración, comprobar que se dispone de una copia de respaldo actualizada.

1. Seleccionar ***Administración del sistema > Salvar/restablecer ajustes***.
2. Seleccionar **Restablecer ajustes de fábrica**.
3. Escribir **Nombre usuario**.
4. Escribir **Contraseña**.
5. Escribir la frase de seguridad, tal y como se muestra (mayúsculas y minúsculas).
6. Hacer clic en **Restablecer ajustes de fábrica**.

   Aparece el siguiente mensaje de advertencia: “"Se está reiniciando el dispositivo" y se muestra una barra de progreso.

   Cuando la barra de progreso llega a su fin, el servidor sale de línea y el navegador muestra la página por default para cuando no puede conectarse a una dirección web.
7. Borrar la caché del navegador. (En Internet Explorer 8 o posterior, pulsar <Ctrl>+<Mayús>+<Supr>.)

   Cuando el servidor está nuevamente en línea, aparece el Formulario de aceptación de licencia de software de usuario final.
8. Hacer clic en **Aceptar**.

Actualización de firmware

El software goEntry se encuentra en la placa de circuitos del controlador. Las actualizaciones periódicas del software se aplican al controlador por medio de la función Actualización de firmware.

1. Abrir el navegador de Internet.
2. Descargar la última actualización del firmware goEntry.
3. Iniciar sesión en goEntry.
   a. Escribir direcciones IP para goEntry en la barra direcciones del navegador.
   b. Si al usar Internet Explorer recibe una advertencia sobre el certificado de seguridad, seleccionar **Pasar a este sitio web (no recomendado)**.
   c. Escribir **Nombre usuario**.
   d. Escribir **Contraseña**.
   e. Seleccionar **Idioma**.
   f. Hacer clic en [Iniciar sesión].
4. Seleccionar ***Administración del sistema > Actualizaciones firmware***.
5. Hacer clic en [Buscar].
6. Navegar y seleccionar archivo actualización del firmware.
7. Hacer clic en [Actualizar].

Reiniciar el controlador del sistema goEntry

1. Seleccionar ***Administración de Sistema > Dispositivos***.
2. En la lista de dispositivos, seleccionar el controlador.
3. Hacer clic en [Reiniciar controlador].

Página Ajustes del sistema

La página Ajustes del sistema se divide en cinco etiquetas. Por default, se exhibe la etiqueta Información del sistema.

Etiqueta Información del sistema

Esta página es meramente informativa y muestra la versión del firmware de aplicación, la versión del firmware de la interfaz de usuario y la versión del firmware del Kernel. La versión del firmware de aplicación y de la interfaz de usuario debe ser la misma.

Usar esta información sobre las versiones para asistencia técnica y para determinar cuándo actualizar a una versión más reciente del firmware.

Etiqueta Fecha y hora

La fecha y la hora se se usan para sincronizar los eventos con los videos correspondientes y para implementar el horario de las puertas y el comportamiento de las lectoras.

Nota: Si se cambia manualmente la hora en el plazo de un minuto de un período programado, o la función NTP lo hace de forma automática, entonces el programa se lleva a efecto inmediatamente en lugar de en el momento designado.

Ver **Configurar la fecha y hora en pág. 12.**

Etiqueta Configuración de red

Esta etiqueta muestra la configuración de red de goEntry. En esta ficha se puede crear un certificado de seguridad para el protocolo seguro de transferencia de hipertexto (https), importar un certificado de seguridad y configurar la dirección del protocolo de internet (IP), máscara de subred, puerta de enlace predeterminada y servidor de nombres de dominio (DNS), según las necesidades de la configuración específica de red de las instalaciones.

Ver **Configuración de seguridad de la red en pág. 13.**

Etiqueta Seguridad

La etiqueta Seguridad de la página Ajustes del sistema permite configurar aspectos relativos a la seguridad física de las instalaciones. La seguridad de la red se configura en la etiqueta Configuración de red.

Ver **Configuración de seguridad en pág. 14.**

Etiqueta Campos definidos por el usuario

Esta etiqueta permite crear campos personalizados en el registro de personas, para organizar su orden en la pantalla y proteger los campos que contienen información confidencial.

El registro de personas en la base de datos de goEntry puede tener campos definidos por el usuario. Esto permite introducir datos personales de los empleados, tales como el número de matrícula del vehículo o el número de teléfono particular. El campo debe estar habilitado para aparecer en la página Personas. Si se deshabilita un campo, se remueve de la base de datos y se pierden los datos correspondientes contenidos en el registro de cada persona.

Ver **Configuración de Campos definidos por usuario en pág. 36.**

Descripción de formatos de tarjeta

Antes de que una credencial pueda ser reconocida, goEntry debe estar configurado para reconocer el formato de la tarjeta, es decir, la forma en que los datos se formatean en la tarjeta de identificación.

goEntry está preconfigurado para reconocer 16 formatos de tarjeta comerciales y es compatible con hasta ocho formatos de tarjeta activos al mismo tiempo. Si el formato de tarjeta usada no figura en la lista, puede agregarse como un tipo personalizado.

Formatos sin procesar (raw)

Un formato sin procesar de tarjeta no incluye el código de instalaciones, sino que trata todos los bits de datos de la tarjeta como parte de la credencial de acceso. Por consiguiente, las credenciales con

formato sin procesar son más fáciles de configurar que las tarjetas que incluyen el código de instalación.

Muchos formatos estándar incluyen el código de instalación como parte de la identificación de la credencial. De modo que aumenta la sofisticación de la configuración de seguridad del lugar, pero también aumenta la complejidad de la configuración. Por ejemplo, si se usa el código de instalación y una puerta entra en modo degradado, porque no puede comunicarse con goEntry, la puerta puede ser configurada para abrirse, si una tarjeta con un código de instalación válido pasa por la lectora. Esto se debe a que el controlador de las puertas no almacena la base de datos completa de las personas, pero puede almacenar el código de instalación.

CAPÍTULO 7 *Solución de problemas*

Borrar caché del navegador de Internet

Borrar la memoria caché y reiniciar el navegador puede resolver muchos problemas aparentes, tales como un repentino comportamiento extraño del softwaregoEntry Los pasos específicos varían según la marca y versión del navegador.

1. Terminar la sesión en goEntry y volver a su página principal.
2. Borrar historial y caché del navegador.
3. Cerrar el navegador y volver a abrirlo.
4. Iniciar sesión en goEntry.

Nota: Tras habilitar o deshabilitar HTTPS/SSL, verificar que se limpió la caché del navegador, especialmente si se usa Firefox o Chrome.

Requisitos de visualización

La aplicación goEntry se ejecuta en un navegador de internet. Para obtener la mejor visualización, se debe:

- Usar Internet Explorer 8 o posterior
- Abrir la ventana del navegador a pantalla completa (un ancho mínimo de al menos 1024 píxeles es necesario para evitar la necesidad de desplazarla)
- Ajustar la resolución de la pantalla a un mínimo de 1024 píxeles de ancho

Capacidades y limitaciones del sistema

Atributo	GOE-
Cantidad de personas	10,000
Cantidad de credenciales individuales	10,000
Credenciales por persona	5
Niveles de acceso	64
Niveles de acceso por credencial	8
Horarios	64
Intervalos de tiempo por horario	6
Grupos de feriados por horario	8
Grupos de feriados	8
Feriados por grupo de feriados	32
Feriados (total)	255
Áreas	64
Grupos de lectoras	64
Roles de operador	32
Campos definidos por el usuario	10
Plantillas de video	64
Formatos de tarjeta	8
Cantidad de eventos mantenidos en registro de eventos	65,000
Puertas/Lectoras	
Cantidad de puertas (controladores de puertas, de tarjeta básica o dual) con lectores de entrada/ cantidad de puertas con lectores de entrada y salida	64 / 32
Módulos duales de control de puertas GOE-ADD-2D-BRD (incluidos los incorporados)	32
Lectoras (total)	64
Entradas/salidas	
Cantidad total de entradas al sistema (incluido el controlador del sistema goEntry)	132
Cantidad total de salidas del sistema (incluido el controlador del sistema goEntry)	66
Número total de Add-Ons de expansión de entrada/salida GOE-ADD-IO o GOE-ADD-IO-BRD	8
Cámaras/DVRs	
DVRs	4
Cámaras por DVR	
TVR10 (EMEA y EE. UU.)	4
TVR30/TVR31 (solo en EE. UU.)	16
Cámaras (máximo)	64

Atributo	GOE-
Puertos Ethernet (total/compatibilidad)	2/1
Puertos de bus de SNAPP RS-485	4

Nota: TVR10 está disponible en los Estados Unidos y Europa, TVR30/TVR31 está disponible solo en los Estados Unidos.

Resumen de roles de operador predefinidos

Niveles de permiso:

- **Ninguno**: El operador no puede visitar ni ver esta página
- **Visión**: El operador puede ver la página o los datos, pero no puede hacer cambios ni ejecutar comandos
- **Modificación / ejecución**: El operador puede modificar la configuración o ejecutar comandos

Permiso	Niveles de permiso	Administra dor	Operador	Guarda	Solo ver	Distribui dor
Niveles de acceso	Ninguno, visualización, modificación	Modificación	Modificación	Visualiza ción	Visualizac ión	Modifica ción
Restablecim iento del Anti-passback	Ninguno, visualización, ejecución	Ejecutar	Ejecutar	Ejecutar	Visualizac ión	Ejecutar
Áreas	Ninguno, visualización, modificación	Modificación	Visualización	Visualiza ción	Visualizac ión	Modifica ción
Base de datos de respaldo	Ninguno, ejecutar	Ejecutar	Ejecutar	Ninguno	Ninguno	Ejecutar
Control de movimiento horizontal, vertical y zoom de las cámaras	Ninguno, ejecutar	Ejecutar	Ejecutar	Ejecutar	Ninguno	Ninguno
Formatos de tarjeta	Ninguno, visualización, modificación	Modificación	Visualización	Ninguno	Ninguno	Modifica ción
Credenciale s	Ninguno, visualización, modificación	Modificación	Modificación	Visualiza ción	Ninguno	Modifica ción
Fecha y hora	Ninguno, visualización, modificación	Modificación	Modificación	Visualiza ción	Visualizac ión	Modifica ción

Permiso	Niveles de permiso	Administrador	Operador	Guarda	Solo ver	Distribuidor
Dispositivos	Ninguno, visualización, modificación	Modificación	Visualización	Visualización	Visualización	Modificación
Diagnóstico	Ninguno, visualización	Visualización	Visualización	Visualización	Visualización	Visualización
Puertas	Ninguno, visualización, ejecución	Ejecutar	Ejecutar	Ejecutar	Visualización	Ejecutar
Eventos	Ninguno, visualización	Visualización	Visualización	Visualización	Visualización	Visualización
Actualización de firmware	Ninguno, ejecutar	Ejecutar	Ninguno	Ninguno	Ninguno	Ejecutar
Feriados	Ninguno, visualización, modificación	Modificación	Modificación	Visualización	Visualización	Modificación
Entrada/salida	Ninguno, visualización, ejecución	Ejecutar	Ejecutar	Ejecutar	Visualización	Ejecutar
Configuración de la red	Ninguno, visualización, modificación	Modificación	Visualización	Visualización	Visualización	Modificación
Funciones de operador	Ninguno, visualización, modificación	Modificación	Visualización	Visualización	Visualización	Visualización
Personas	Ninguno, visualización, modificación	Modificación	Modificación	Visualización	Visualización	Modificación
Campos de usuario protegidos	Ninguno, visualización, modificación	Modificación	Ninguno	Ninguno	Ninguno	Ninguno
Grupos de lectoras	Ninguno, visualización, modificación	Modificación	Modificación	Visualización	Visualización	Modificación
Reportes	Ninguno, ejecutar	Ejecutar	Ejecutar	Ejecutar	Ejecutar	Ejecutar
Restablecer configuración	Ninguno, ejecutar	Ejecutar	Ninguno	Ninguno	Ninguno	Ejecutar
Restaurar base de datos	Ninguno, ejecutar	Ejecutar	Ninguno	Ninguno	Ninguno	Ejecutar

Permiso	Niveles de permiso	Administrador	Operador	Guarda	Solo ver	Distribuidor
Horarios	Ninguno, visualización, modificación	Modificación	Modificación	Visualización	Visualización	Modificación
Seguridad	Ninguno, visualización, modificación	Modificación	Visualización	Visualización	Visualización	Modificación
Información del sistema	Ninguno, visualización	Visualización	Visualización	Visualización	Visualización	Visualización
Cuentas de usuario	Ninguno, visualización, modificación	Modificación	Visualización	Ninguno	Ninguno	Modificación
Campos definidos por usuario	Ninguno, visualización, modificación	Modificación	Modificación	Visualización	Visualización	Modificación
Video	Ninguno, visualización	Visualización	Visualización	Visualización	Visualización	Ninguno
Plantillas video	Ninguno, visualización, modificación	Modificación	Modificación	Visualización	Visualización	Modificación

Diagnóstico

goEntry proporciona información de diagnóstico, no hay acciones que se puedan realizar para ejecutar pruebas específicas de diagnóstico. La página Diagnóstico cuenta con indicadores visuales de las fallas más comunes para ayudar a identificar y resolver problemas. Toda la información se puede consultar desde el momento de inicio de sesión y en cualquier momento a partir de entonces. Se pueden actualizar manualmente los datos haciendo clic en [Actualizar]. La página muestra la última vez que se actualizó la pantalla.

Nota: El controlador del sistema goEntry no puede mostrar una lectura precisa de la intensidad de la corriente continua cuando el sistema está alimentado por una fuente de CC. La información de la intensidad de la CC solo se mostrará cuando el controlador del sistema goEntry se alimenta con CA.

Diagnóstico	Valor mostrado	Estado
Alimentación de CA	Correcta | Baja | Falla	INF = Correcto WRN = Baja ERR = Falla

Diagnóstico	Valor mostrado	Estado
Alimentación de CC	Tensión, Intensidad	INF >= 10.0 VWRN < 10.0 V WRN = sobrecarga de intensidad
Batería de respaldo	Tensión, intensidad, carga | descarga	INF >= 11,7 VWRN < 11,7 V ERR < 11,4 V, sin batería
Batería de la memoria	Tensión	INF >= 2,3 V WRN < 2,3 V ERR < 2,0 V
Fusibles	Correcto | *Nombre del fusible, ...*	INF = Todos OK ERR = Si alguno no está correcto
Controlador	Correcto | *Problemas*,...	INF = Correcto WRN = Si no está correcto
Módulos	OK | *ModuleName problema*,...	INF = Todos OK WRN = Si hay sabotaje ERR = Si fuera de línea
Puertas	OK | *DoorName problema*,...	INF = Todos OK WRN = Si sujetada, forzada, saboteada ERR = Si fuera de línea
Entradas digitales	Correcta | *InputName problema*,...	INF = Todos OK WRN = Si hay sabotaje ERR = Si fuera de línea
Tiempo en actividad	Hora del último arranque, días funcionando	INF = Siempre
Carga prom. CPU	1 m, 5 m, 15 m	INF 15 m < 0.80 WRN 15 m >= 0.80 ERR 15 m >= 0.95
Uso de memoria	Usado, total	INF < 95 % WRN >= 95 % ERR = 100%
Almacenamiento principal	Porcentual	INF < 90% WRN >= 90% ERR = 100%

Diagnóstico	Valor mostrado	Estado
Almacenamiento imágenes y respaldo	Usado, total	INF < 50% WRN >= 50% ERR >= 95 %
Tarjetas ADP	Usado, total	INF = Siempre
Puertas	Usado, total	INF = Siempre
Lectoras	Usado, total	INF = Siempre
Tarjetas E/S mejorada	Usado, total	INF = Siempre
Entradas	Usado, total	INF = Siempre
Salidas	Usado, total	INF = Siempre
DVRs	Usado, total	INF = Siempre
Cámaras	Usado, total	INF = Siempre
Persona	Usado, total	INF = Siempre
Credenciales	Usado, total	INF = Siempre
Niveles de acceso	Usado, total	INF – Siempre
Horarios	Usado, total	INF – Siempre
Grupos de feriados	Usado, total	INF – Siempre
Feriados	Usado, total	INF = Siempre
Áreas	Usado, total	INF = Siempre
Grupos de lectoras	Usado, total	INF = Siempre
Funciones de operador	Usado, total	INF = Siempre
Plantillas video	Usado, total	INF = Siempre
Formatos de tarjeta	Usado, total	INF = Siempre

Fusibles

Los fusibles protegen la alimentación de CC suministrada por la tarjeta del controlador del sistema goEntry para su uso por los periféricos externos.

Fusible	+V	0V
Aux. 1	CN3.1	CN3.2
Aux. 2	CN3.3	CN3.4

Fusible	+V	0V
Controlador de puerta	CN10.2 CN17.2	CN11.4 CN18.4
Entrada auxiliar	CN21.1	CN21.3 CN22.2

Estados problemas de hardware

Los items de hardware pueden tener los siguientes problemas:

Controlador

- Sabotaje

Módulos

- Fuera de línea
- Sabotaje

Puertas

- Fuera de línea
- Forzadas
- Sujetadas
- Sabotaje solicitud de salida
- Sabotaje contacto puerta
- Sabotaje dispositivo aux puerta
- Sabotaje puerta

Entrada digital:

- Fuera de línea
- Sabotaje

Mensajes error, advertencia y eventos

Estados de sabotaje

El controlador del sistema goEntry no distingue la entrada de cuál de las cuatro entradas de puerta está en estado de sabotaje, al registrar los eventos de sabotaje. El estado en tiempo real de sabotaje en tiempo real de las entradas se puede ver en la página Diagnóstico o usando el asistente de instalación.

Eventos de alimentación y baterías

El controlador del sistema goEntry se apaga cuando el sistema está alimentado por batería

Si el controlador se alimenta exclusivamente de la batería y la tensión de la batería cae a menos de 10.2 voltios, el controlador se apaga hasta que se restaura la alimentación de CA.

Ver **Eventos batería de respaldo en pág. 71.**

Eventos alimentación de CA

Código evento	Descripción evento
Evento 14626	Falla alimentación CA
Evento 14627	Alimentación CA restaurada

Nota: El controlador del sistema goEntry no puede mostrar una lectura precisa de la intensidad de la corriente continua cuando el sistema está alimentado por una fuente de CC. La información de la intensidad de la CC solo se mostrará cuando el controlador del sistema goEntry se alimenta con CA.

Eventos batería de respaldo

Los eventos de la batería de respaldo se producen cuando la tensión de la batería de respaldo cae por debajo de determinados umbrales.

Código evento	Descripción evento	Causa
Evento 14612	Batería de respaldo crítica	La tensión cae a menos de 11.4 V o sube a más de 10.2 V
Evento 14613	Corte de batería de respaldo	La tensión cae a menos de 10.2V o sube a más de 9.0V
Evento 14624	Batería de respaldo baja	La tensión cae a menos de 11.7V o sube a más de 11.4V
Evento 14625	Batería de respaldo restaurada	La tensión sube a más de 11.7 V
Evento 14649	No se detecta batería de respaldo	La tensión cae a menos de 9.0 V

Nota: Si el sistema se alimenta exclusivamente de la batería de respaldo, se apagará a 10.2 V y no se generarán los eventos de corte y no detección.

Evento batería de memoria

Código evento	Descripción evento
Evento 14618	Batería respaldo de memoria baja

Eventos fusibles

Código evento	Descripción evento
Evento 14651	Fusible cortado
Evento 14652	Fusible restaurado

Eventos dispositivos

Código evento	Descripción evento	Dispositivo
Evento 4105	Comunicaciones del dispositivo en falla	Controlador de puerta, expansor E/S
Evento 4106	Comunicaciones dispositivo restauradas	Controlador de puerta, expansor E/S
Evento 4107	Alarma sabotaje*	Controlador, controlador puerta, expansor E/S
Evento 14622	Problema de sistema	Controlador
Evento 14623	Sistema restaurado	Controlador
Evento 14628	Dispositivo falló	Controlador
Evento 14629	Dispositivo restaurado	Controlador
Evento 14643	Sabotaje restaurado*	Controlador, controlador puerta, expansor E/S

* No se aplica a controladores de puerta integrados

Comunicaciones del dispositivo en falla/restauradas
Se usa para indicar los errores de comunicación con dispositivos instalados más adelante. Se produce cuando se pierde o se establece la comunicación del bus de SNAPP con un dispositivo configurado, instalado más adelante. El dispositivo siempre muestra cuál es el módulo afectado.

Dispositivo en falla/restaurado
Se usa para indicar problemas en general de los dispositivos instalados más adelante. Se produce cuando cualquier entrada de sabotaje del dispositivo cambia de estado (incluido el sabotaje externo/pared, pero no el sabotaje a la puerta), o cuando se detecta un error de comunicación por VBUS. El dispositivo siempre indica el controlador. Para cada evento de sabotaje, habrá un evento de sabotaje correspondiente para el dispositivo. Para los eventos de error de VBUS, no hay forma de informar cuál dispositivo tiene el error de VBUS, por lo que no hay ningún evento correspondiente que muestre cuál es el dispositivo afectado.

Problema de sistema/restaurado
Se usa para indicar problemas en general del sistema. Se produce cuando el **sabotaje externo/a la pared** cambia de estado. El **dispositivo** siempre indica el controlador. Este evento puede usarse en el futuro para identificar otras condiciones de problemas.

Eventos sabotaje de puerta

Código evento	Descripción evento
Evento 14633	Sabotaje de puerta restaurado
Evento 14632	Alarma sabotaje de puerta

Alarma sabotaje de puerta/restaurada
Se usa para indicar la condición de sabotaje de cualquiera de las cuatro entradas de las puertas: DR, RTE, TR, AUX. El evento de alarma de sabotaje se genera al detectar una condición de sabotaje en cualquiera de las entradas, o cuando TR está activo. No se generarán otros eventos de alarma de sabotaje para RTE, TR y AUX hasta que todas las condiciones de sabotaje que se resuelvan, pero se generarán otros eventos de alarma de sabotaje para DR, aunque las otras condiciones de sabotaje se mantengan. El evento de sabotaje restaurado solo se genera cuando se resuelve la condición de sabotaje de las cuatro entradas y TR está inactivo

Eventos de entrada auxiliar

Código evento	Descripción evento
Evento 14640	Entrada activa
Evento 14641	Alarma de sabotaje de entrada
Evento 14642	Entrada inactiva
Evento 4170	Entrada deshabilitada

Eventos de salida auxiliar

Código evento	Descripción evento
Evento 10240	Salida activada
Evento 11264	Salida desactivada

Advertencia "Objetos han cambiado"

De vez en cuando la caché del navegador local puede perder la sincronización con goEntry. En este caso, la interfaz se deshabilita y aparece el mensaje de advertencia.

Hacer clic en el texto de la advertencia para recargar la página.

Evento "Error de sinc. NTP"

La sincronización temporal con el servidor NTP requiere el acceso desde el panel al servidor NTP a través del puerto UDP 123. Si este puerto no está accesible, la hora del panel no se sincroniza con el servidor NTP y se registran eventos de "Error de sinc. NTP".

Errores de Active X reproductor de video

Ninguna conexión de video activa

Este mensaje aparece en la página ***Monitoreo > Video*** y el panel Detalle de eventos de la página ***Eventos***.

El mensaje puede significar lo siguiente:

- no se ha configurado un dispositivo de cámara
- la aplicación goEntry ha perdido la comunicación con una DVR conectada
- el control ActiveX necesario para ver el video no se ha instalado o está desactualizado

Nota: El video solo puede verse en Internet Explorer.

Si el mensaje de error aparece al hacer clic en el icono de una cámara al lado de un evento:

1. Hacer clic en [Reproducir video del evento].
2. El video se exhibe o el control ActiveX se instala.
3. Si no sucede nada y el mensaje permanece, verificar el funcionamiento de la cámara y la DVR:
    a. Ver **Configuración de dispositivos de video en pág. 25.**
    b. Ver **Enlazar las cámaras a los dispositivos de rastreo de videos de eventos en pág. 27.**.

Si el mensaje de error aparece al seleccionar *Monitoreo > Video*:

1. Hacer doble clic en el panel de video que muestra el mensaje de error.
2. Si el video no aparece:
    a. Seleccionar ***Monitoreo > Plantillas de video***.
    b. Seleccionar la plantilla de video que se estaba viendo.
    c. Comprobar que se selecciona la cámara correcta en cada lista desplegable de cada panel de la plantilla de video.
3. Si la cámara correcta no figura en la lista, verificar si la cámara se agregó a la página Dispositivos y está funcionando:
    a. Ver **Configuración de dispositivos de video en pág. 25.**
    b. Ver **Añadir una cámara de video en pág. 26.**
    c. Ver **Agregar plantillas de video en pág. 27.**

El navegador de internet no consigue cargar la página Inicio de sesión

Tras cambiar entre el protocolo de hipertexto seguro (HTTPS) y el normal (HTTP), puede suceder que Firefox o Chrome no carguen la página de inicio de sesión del Controlador del sistema goEntry.

Ver **Borrar caché del navegador de Internet en pág. 63.**

Glosario

Nivel de acceso
Una o más combinaciones de lectora/horario, que se usa para controlar el acceso de los tarjetahabientes al hardware. Los niveles de acceso pueden asignarse a tarjetas de identificación activas para definir a qué lectoras y en qué horario la tarjeta tiene acceso.

ANSI
Siglas de American National Standards Institute, una organización voluntaria que establece normas para la industria informática.

APB
Siglas de Anti-passback. Impedimento de que una tarjeta de identificación entre en un sistema de control de acceso si ha entrado recientemente en la misma lectora o área (Anti-passback cronometrado) o se considera que no está en el área adecuada para poder entrar en la nueva área (Anti-passback por área). En pocas palabras, se trata de un método de monitoreo de las entradas y salidas de los tarjeta habientes para garantizar que no se transfiere la tarjeta para que otra persona tenga acceso.

Área APB
Las áreas son definidas por las lectoras por las que se entra y sale. Se registra el Área en que una tarjeta se encuentra. Cuando una tarjeta trata de entrar en una área determinada a través de una lectora determinada, se niega el acceso si no está registrada como estando en el área en la que la que se encuentra la lectora en la que está configurada su salida.

Tipo de Tarjeta
Clasifica las tecnologías de codificación de las tarjetas, tales como magnética, Wiegand, tarjeta inteligente, First Access, etc.

DHCP
Siglas de Dynamic Host Configuration Protocol (Protocolo de configuración dinámica de host). Protocolo de comunicaciones que permite a los administradores de red administrar de forma centralizada y automatizar la asignación de direcciones de Protocolo de Internet en la red de una organización.

Contacto de puerta
Dispositivo de dos piezas usado por un sistema de acceso por tarjeta para indicar si una puerta está abierta o cerrada. Por lo general, una pieza está montada en la puerta y la otra en una posición similar en el marco de la puerta.

Sujetador de puerta

Dispositivo que sujeta la puerta en la posición abierta hasta que el sistema lo instruye a cambiar de estado.

Apertura

Dispositivo eléctrico o magnético que se usa para mantener la puerta en la posición cerrada. La apertura de una cerradura eléctrica requiere algún tipo de carga eléctrica generada por otro dispositivo, tal como una lectora de tarjetas.

Ethernet

Norma de redes de comunicación LAN que usan cable coaxial o par trenzado. IEEE 802.3 es la norma para Ethernet. Existen los siguientes tipos de Ethernet: 10 Mbps (Mega [millones] bits por segundo), 100 Mbps, 1 Gbps (Giga [mil millones] bits por segundo)

Código de instalación

Campo opcional en la tarjeta que identifica inequívocamente un lugar. Los proveedores de tarjetas Wiegand suelen proporcionar el código de instalación y lo almacenan en las tarjetas. En otras tarjetas, el usuario define el código de instalación. Una lectora de tarjetas puede ponerse en modo de Solo Código de Instalación, lo que requiere el código de instalación antes de que se autorice el acceso.

HTTP

Siglas de Hyper Text Transfer Protocol (Protocolo de transferencia de hipertexto) Define la forma en que se formatean y transmiten los mensajes y controla las acciones que los servidores y navegadores web deben ejecutar en respuesta a distintos comandos.

IP

Siglas de Internet Protocol (Protocolo de Internet), que especifica el formato de los paquetes y el esquema de direccionamiento en una red.

Dirección IP

Identificador de una computadora en una red TCP/IP. El formato de una dirección IP es una dirección numérica de 32 bits, escrita como cuatro números separados por puntos. Cada número puede estar entre cero y 255. Por ejemplo, 1.120.4.72 podría ser una dirección IP.

Cámara IP

Una cámara de video digital que se conecta directamente a la red con su propia dirección IP y tiene capacidad para transmitir imágenes usando protocolos de comunicación normalizados, tales como TCP/IP. Una cámara IP no necesita estar conectada a una PC ni a una tarjeta de captura de vídeo.

LAN

Siglas de Local Area Network (red de área local). Conexión por cables de alto rendimiento de las computadoras personales dentro de un área limitada, para que los usuarios puedan intercambiar información, compartir periféricos y usar los recursos de una unidad de almacenamiento secundario masivo llamado servidor de archivos.

LDAP

Siglas de Lightweight Directory Access Protocol (protocolo ligero de acceso a directorios), LDAP, es un protocolo de software usado comúnmente para hablar con los servidores que almacenan la información

de usuario, incluidos los certificados digitales. Permite que cualquiera localice organizaciones, personas y otros recursos, tales como archivos y dispositivos en una red, ya sea por internet o en una intranet corporativa. La conexión a un servidor LDAP puede ser no encriptada o encriptada con SSL.

National Television Standards Committee

Comúnmente conocida como NTSC, es la señal de televisión usada en los Estados Unidos y Japón.

PAL

Norma de video usada en Europa, Australia y Nueva Zelanda. El sistema PAL transmite 625 líneas por 1/25 segundos.

PIN

Siglas de Personal Identification Number (número de identificación personal), un número generalmente asociado con una persona y usado en el control de acceso

PTZ

Siglas de Pan-Tilt-Zoom (movimiento horizontal, vertical y zoom). Una característica de las cámaras cuyo movimiento horizontal, vertical y zoom se puede controlar por computadora. PTZ permite aumentar el área de visualización de una cámara porque es posible girarla en diferentes direcciones.

Enrutador

"Hub" inteligente que permite que varias subredes se conectan entre sí para compartir datos y recursos

SNMP

Siglas de Simple Network Management Protocol (Protocolo simple de administración de redes). Método de gestión de varios elementos de hardware, por ejemplo, una impresora, conectada a la red.

SSL

Siglas de Secure Sockets Layer (Capa de sockets seguros), un protocolo común para la autenticación y comunicación cifrada a través de internet. SSL se usa en la comunicación con servidores web (HTTP) y LDAP.

Subred

Grupo de computadoras que comparten las mismas propiedades y recursos de red

Supervisada

Puerta o gabinete cableado con un circuito de continuidad, de modo de detectar intentos de sabotaje.

TCP/IP

Siglas de transmission Control Protocol/ Internet Protocol (Protocolo de control de transmisión/Protocolo de Internet). Conjunto de protocolos de comunicación usado para conectar servidores a través de Internet.

Puerto TCP/IP

Cada proceso que quiere comunicarse con otro proceso se identifica al conjunto de protocolos TCP/IP a través de uno o más puertos. Un puerto es un número de 16 bits, usado por el protocolo host a host para identificar a qué protocolo de nivel superior o programa de aplicación (proceso) debe entregar los mensajes entrantes.

No supervisada

Puerta o gabinete que no está cableado con un circuito de continuidad para detectar intentos de sabotaje.

URL

Siglas de Uniform Resource Locator (Localizador uniforme de recursos). URL es la dirección de un recurso o un archivo disponible en una red TCP/IP, tal como internet.

Wiegand

Tecnología de control de acceso mediante tarjetas que contienen cables de tungsteno cargados magnéticamente, cortados en tiras y montados verticalmente en columnas.

Asistente

Programa utilitario que se usa como guía para trabajar paso a paso a través de un proceso.

Índice

Símbolos

.NET ... 7
.NET 4.0 ... 26

Numéricos

1 Gbps ... 78
10 Mbps ... 78
100 Mbps ... 78
100BaseT ... 6

A

á ... 28
Acceso de discapacitados ... 19
Activado/desactivado ... 25
Activar
    credencial ... 42
ActiveX ... 26
Activo desde ... 41
Activo hasta ... 41
Admin ... 65
Administrador ... 35
    cambiar la contraseña de ... 8
    cuenta usuario ... 8
Advertencia
    Objetos han cambiado ... 73
Advertencias
    Se está reiniciando el dispositivo ... 59
Alarma de sabotaje habilitada ... 25
Alarma sabotaje de puerta ... 73
Alimentación CC ... 69
Añadir
    área ... 28
    cámara de video ... 26
    campos definidos por usuario ... 36
    credencial ... 39
    cuentas usuario ... 39
    Formatos de tarjeta ... 16
    Fotos de identificación ... 40
    grabadora digital de video ... 26
    grupos de feriados ... 29
    grupos de lectoras ... 33
    horarios ... 31
    niveles de acceso ... 34
    personas ... 39
    plantillas de video ... 27
    roles de operador ... 35
Ancho de banda del flujo de video ... 26
ANSI ... 77
Anti-passback ... 23, 27, 28, 47, 55
    configuración ... 29
APB ... 77
Apertura ... 78
Apertura automática ... 23
Área APB ... 77
Área de llegada ... 28
Área de partida ... 28
Área por default ... 28
Asistente ... 79
Asistente de detección e instalación ... 7
Asistente de importación/exportación ... 7

B

Bloquear al cerrar ... 22
Bloqueo magnético ... 15, 21
Botón Importar certificado ... 14
Búsqueda
    personas ... 45

C

Caché del navegador ... 63
Caja de diálogo Cargar certificado ... 14
Caja de diálogo Remover
        item ... 16, 28, 31, 33, 34, 40, 42
Caja de diálogo Respaldo
        de la base de datos ... 58
Caja de diálogo Solicitud de firma de
        certificado. ... 13
Caja de selección Desbloquear todas las
        puertas ... 17, 25
Caja de selección puede iniciar sesión. ... 44
Caja selecc. Protegido ... 36
Caja Utilizar tiempo extendido de apertura 41
Cámara enlazada ... 17, 20, 21, 24, 25, 27
Cámara IP ... 78
Cámaras PTZ ... 26
Cambiar
    contraseñas ... 43
Campo exclusivo ... 36
Campos definidos por usuario
    protegido ... 36
Cargar
    fotos ... 40
Código de emisión ... 16
Código de instalación ... 16, 78
Configuración y control del
        navegador web ... 26
Configurar
    anti-passback ... 29
    área ... 28
    áreas ... 27, 28
    cámara de video ... 25, 26
    campos definidos por usuario ... 36
    controlador goEntry ... 7
    credencial ... 39
    cuentas usuario ... 39
    dispositivos ... 27
    DVR ... 25, 26
    fecha y hora ... 12, 74
    Formatos de tarjeta ... 16
    grupos de lectoras ... 33

horarios 31
lectoras 24
niveles de acceso 34
opciones de puerta 22
Página Personas 36
personas 39
plantillas de video 27
puerta 19
puertas 18
roles de operador 35
sincronización temporal con el servidor NTP 12, 74
video de evento 27
Contacto de puerta 20, 21, 77
Contraseñas
cambio 43
Convenciones 1
Credencial
activar 42
de duración limitada 42
desactivar 42
perdida o robada 42
reporte 44
Credencial ID 38
Credencial y PIN 24, 54
Credenciales 38
administración 39
CSV 38
Cuentas usuario
administración 39
permisos de grupo 36

D

Datos confidenciales
proteger 36
Datos cuenta usuario 38
De uso general
entradas 8, 17, 18
salidas 8, 17, 18
Desactivar
credencial 42
Desbloqueo programado 23
DHCP 77
Dirección IP 8, 13
Dispositivos de video 26
Distribuidor 35, 65
Drive CD/DVD 7
Duración de la reproducción previa al evento 26
DVR 12

E

Enrutador 79
de red 6
Entrada auxiliar 23
Entradas
auxiliares 55
monitoreo 55
Error de sinc. NTP 12, 74
Errores de Active X 74
Ethernet 6, 78
Etiqueta Campos definidos por usuario 36, 61
Etiqueta Configuración de red 13, 14, 61
Etiqueta Configuración del sistema 14
Etiqueta Cuenta de Usuario 43, 44
Etiqueta Entradas 25
Etiqueta Fecha y hora 60
Etiqueta General 17
Etiqueta Información del sistema 60
Etiqueta Seguridad 14, 61
Etiqueta Ver horarios 37
Evento 10240 73
Evento 11264 73
Evento 14612 71
Evento 14613 71
Evento 14618 72
Evento 14624 71
Evento 14625 71
Evento 14640 73
Evento 14641 73
Evento 14642 73
Evento 14644 53
Evento 14646 53
Evento 14649 71
Evento 14651 72
Evento 14652 72
Evento 4170 73
Eventos

credenciales perdidas o robadas 42
Error de sinc. NTP 12, 74
exportación 48
video 49
video de 27
visualización 48
Eventos alimentación de CA
Evento 14626 71
Evento 14627 71
Eventos batería de respaldo 71
14612 71
14613 71
14624 71
14625 71
14649 71
Eventos de entrada auxiliar
14640 73
14641 73
14642 73
4170 73
Eventos de salida auxiliar
10240 73
11264 73
Eventos dispositivos
Evento 14622 72
Evento 14623 72
Evento 14628 72
Evento 14629 72
Evento 14643 72
Evento 4105 72
Evento 4106 72
Evento 4107 72
Eventos sabotaje de puerta
Evento 14632 73
Evento 14633 73
Exento de Anti-passback 41
Exportar
eventos 48

F
Fecha 12
Feriados
personalizados 30
que se repitan todos los años 30
únicos 30
Filtro
lista de personas 45
First Access 77
Formatos de tarjeta
Configurar 16
Formulario de aceptación de licencia de software de usuario final 59
Fotos de identificación 40
Fusibles 69

G
Guarda 35, 65

H
Habilitar conexión HTTPS 14
Hoja de propiedades Propiedades de red 14
Hora 13
Horarios
intervalos de tiempo 31
HTTP 78
HTTPS 8, 14, 79
https 61

I
ID Credencial 38
ID personal 36
IEEE 802.3 78
Ingresar en el campo nueva contraseña 43
Instalar Microsoft .NET Framework 4.0. 7
Intentos de PIN 15
Internet Explorer 59, 74
versiones anteriores a 8.0 45
Intervalos de tiempo 31
Introducción 1
IP 6

L
LAN 6, 78
LDAP 78, 79
Lectora para entrar y lectora para salir 23
Lectora solo para entrar 23
Lectoras de credenciales USB 41
Longitud máxima del PIN 14, 15

M
Magnética 77
Máscara de subred 61
Mensajes
Alarma de sabotaje de entrada 73
Alarma sabotaje 72
Alimentación CA restaurada 71
Batería de respaldo baja 71
Batería de respaldo crítica 71
Batería de respaldo restaurada 71
Batería respaldo de memoria baja 72
Comunicaciones del dispositivo en falla 72
Comunicaciones dispositivo restauradas 72
Corte de batería de respaldo 71
Dispositivo falló 72
Dispositivo restaurado 72
Entrada activa 73
Entrada deshabilitada 73
Entrada inactiva 73
Error de sinc. NTP 12, 74
Falla alimentación CA 71
Fusible cortado 72
Fusible restaurado 72
Ninguna conexión de video activa 74
No se detecta batería de respaldo 71

Objetos han cambiado ... 73
Problema de sistema ... 72
Sabotaje restaurado ... 72
Salida activada ... 73
Salida desactivada ... 73
Se está reiniciando el dispositivo ... 59
Sistema restaurado ... 72
Modo de cerradura ... 19, 21, 23
Modo de horario ... 38
Bloqueada ... 38
Credencial y PIN ... 38
Desbloqueada ... 38
lectora ... 54
Primera entrada con tarjeta ... 38
puerta ... 54
Solo credencial ... 38
Modo Puerta degradada ... 15
Código de Instalación ... 15
Restringido ... 15
Todos ... 15
Monitorear
entradas ... 55
puertas ... 38
salidas ... 55

N

National Television Standards Committee . 79
Nivel de acceso ... 38, 77
Niveles de permiso ... 65
No supervisada ... 24, 79
Nombre del dispositivo ... 17
Normalmente abierto ... 24
Normalmente cerrado ... 24
NTP ... 61
NTSC ... 79
Número de empleado ... 36
Número de ID ... 36
Número de identificación exclusivo ... 36
Número de identificación personal (PIN) ... 14
Número de registro en base de datos ... 36
Número de serie ... 5, 17

O

Opciones de lectoras ... 24
credencial y PIN ... 24
solo credencial ... 24
Operador ... 35, 65

P

Página Actualización de firmware ... 60
Página Ajustes del sistema ... 13, 14, 15, 36
Página Asignación de lectoras ... 28
Página Definición de áreas ... 28
Página Diagnóstico ... 67
Página Dispositivos ... 16, 38, 60
Puerta ... 53
Página Entradas/salidas ... 55
Página Eventos ... 47, 49, 74
Página Feriados ... 29
Página Formatos de tarjeta ... 15, 16, 55
Página Grupos de lectoras ... 33
Página Horarios ... 31, 33, 54
Página Niveles de acceso ... 31, 33, 34, 38
Página Personas 36, 39, 40, 43, 44, 45, 61
configurar campos definidos
por usuario ... 36
Panel Credenciales ... 29
Página Plantillas de video ... 27
Página Puertas ... 31
Etiqueta Ver horarios ... 37
Página Roles operador ... 35, 36
Página Salvar/restablecer ajustes ... 59
Página Video ... 49, 50, 74
PAL ... 79
Panel Credenciales ... 29
Período normal de acceso autorizado ... 22
Permisos de grupo
roles operador, ejemplo de ... 36
Personas
administración ... 39
buscar ... 45
credencial ... 39
cuenta usuario ... 39
fotos ... 40
removiendo ... 40
Personas con discapacidad ... 41
PIN ... 38, 79
Proteger datos confidenciales ... 36

protocolo de internet 61
PTZ 79
Puerta
no supervisada 79
supervisada 79
Puerta de enlace predeterminada 61
Puerta mantenida abierta 22
Puerta mantenida/forzada 19, 21, 24
Puertas
Etiqueta Ver eventos 53
Etiqueta Ver horarios 53
menús de comandos 53
monitoreo 38
Puerto TCP/IP 79

R

Red de área local 6
Registros personales
ID exclusiva 36
Reiniciar
controlador goEntry 14
Reiniciar el controlador 60
Relé auxiliar 19, 23
Remover
área 28
credencial 42
Formatos de tarjeta 16
grupo de feriados 31
grupos de lectoras 33
horarios 33
niveles de acceso 34
persona 40
roles de operador 36
Reporte Acceso a lectoras 44
Reporte de nómina 27, 44
Reporte Historial de acceso 44
Reporte lista de asistencia 44
Reportes
Acceso a Lectoras 44
Credencial 44
Historial de acceso 44
Lista de Asistencia 44
Nómina 44
Respaldo 38
Restablecimiento del Anti-passback 55
Restaurar 38
Restaurar ajustes personalizados 59
RF IDeas 41
RFID 41
RJ-45 6

S

Sabotaje 8, 20, 21
Sabotaje de puerta restaurado 73
Salidas
auxiliares 55
monitoreo 55
Seguridad 15
Sensor de conexión del
bloqueo magnético 21, 22
Servicios de Impresión Bonjour 7
Servidor de nombres de dominio (DNS) 61
Servidor NTP 13
SNMP 79
Solicitud de salida (RTE) 19, 20, 21, 22
Solicitud de salida (RTE)
extendida 19, 20, 21, 23
Solo credencial 24, 54
Solo ver 35, 65
SSL 79
start.hta 7
Subred 79
Sujetador de puerta 78
Supervisada 24, 79

T

Tarjeta Inteligente 77
TCP/IP 79
Tensión 71
Terminaciones EOL de entrada 15
Terminaciones EOL de entrada global 8
Tiempo activación relé Aux. 20, 24
Tiempo de bloqueo de PIN 15
tiempo extendido mantenido/abierto 22
Tipo de Tarjeta 77
Tipos de entrada
no supervisada 24
normalmente abierto 24
normalmente cerrado 24
supervisada 24
TVR10 ..... 25, 26
TVR30/TVR31 ..... 25, 26

U

UDP 12, 74
URL 79
USB 41
usuario 37

V

Valores Separados por Comas 38, 48
Versión del firmware de aplicación 60
Versión del firmware de la interfaz de usuario
60
Versión del firmware del kernel 60
Video
controles del reproductor 50
reproducción 49
visualización de eventos 49
Video en directo 49
Video grabado 49

W

Wiegand 77, 79